E-government

Frank ROBBEN
Administrateur-generaal
Kruispuntbank van de Sociale Zekerheid
Frank.Robben@ksz.fgov.be

1. E-government: een structureel hervormingsproces

E-government heeft als doel de dienstverlening van de overheid en de beleidsvoering voortdurend te verbeteren door interne en externe processen en relaties om te vormen met behulp van informatie- en communicatietechnologie. De interne processen en relaties zijn deze binnen elke overheidsinstelling, tussen de overheidsinstellingen en hun personeel en tussen de overheidsinstellingen onderling. De externe processen en relaties zijn deze tussen de overheidsinstellingen enerzijds en de burgers, de ondernemingen en hun vertegenwoordigers anderzijds.

De informatie- en communicatietechnologie is enkel een middel. E-government is een structureel hervormingsproces, dat gebaseerd dient te zijn op een multidisciplinaire aanpak. In deze bijdrage wordt een overzicht gegeven van een aantal belangrijke vereisten voor een doeltreffend E-government:

- het beschouwen van informatie als een strategische productiefactor voor de werking van de overheid;
- een gebruikersgerichte re-engineering van de bedrijfsprocessen en de uitbouw van waardeketens;
- een interoperabiliteitsframework;
- een geïntegreerd informatieveiligheidsbeleid;
- een aangepast jurdisch kader.

Daarna wordt ingegaan op twee Belgische verwezenlijkingen op het vlak van E-government die internationaal worden erkend als best practice: de procesherziening in de sociale sector onder coördinatie van de Kruispuntbank van de Sociale Zekerheid en de elektronische identiteitskaart.

2. Het beschouwen van informatie als een strategische productiefactor voor de werking van de overheid

Informatie is van cruciaal belang voor de goede werking van de meeste overheidsinstellingen: overheidsinkomsten zoals belastingen en sociale-zekerheidsbijdragen zijn afhankelijk van informatie omtrent de inkomsten van burgers en ondernemingen, verkiezingen worden georganiseerd op basis van informatie over de bevolking, rechten en voordelen worden toegekend in functie van de leefomstandigheden van de rechthebbenden en hun omgeving, … Het is dus van groot belang dat de overheidsinstellingen informatie beschouwen als een strategische productiefactor en de nodige zorg besteden aan een effectief en efficiënt beheer ervan. In dat verband stellen we de naleving voor van een aantal basisprincipes op vijf vlakken.

2.1. Informatiemodellering

De omgang met informatie moet worden gebaseerd op een geharmoniseerd informatiemodel. Dat model moet de voor de werking van de overheid benodigde informatie-elementen, hun kenmerken en hun onderlinge relaties beschrijven op een eenduidige wijze. Het informatiemodel sluit best zo nauw mogelijk aan bij de reële wereld. Dit houdt in dat de definitie van de informatie-elementen, van hun kenmerken en van hun onderlinge relaties gebaseerd is op een abstractie van de realiteit, en niet op juridische begrippen. Hierdoor worden wijzigingen aan het informatiemodel als gevolg van wijzigingen aan de wetgeving vermeden.

De informatiemodellering moet zo veel mogelijk rekening houden met de voorzienbare gebruiksbehoeften. Dit veronderstelt een voldoende inzicht in de werking van de verschillende overheidsinstellingen, en kan worden bekomen door de oprichting van een modelleringscomité dat het informatiemodel en de wijzigingen eraan beheert.

Bij het proces van informatiemodellering moet bijzondere aandacht worden besteed aan het temporeel aspect. De benodigde informatie kan betrekking hebben op de situatie op een bepaald ogenblik (bv. het verblijfsadres op 1 januari van een bepaald jaar) of op de situatie gedurende een periode (bv. het loon verdiend tijdens een kwartaal). Het is belangrijk over de overheidsinstellingen heen voldoende consistent te zijn m.b.t. de tijdstippen waarop en de referteperiodes waarvoor informatie nodig is voor de verschillende doeleinden, zoniet wordt een hergebruik van de informatie gehinderd.

De reële wereld verandert voortdurend en niet alle gebruiksbehoeften kunnen voorspeld worden. Bijgevolg moet het mogelijk zijn om het informatiemodel op een flexibele wijze uit te breiden en aan te passen wanneer de reële wereld of het gebruik van de informatie wijzigt.

2.2. Eenmalige inzameling en hergebruik van informatie

Informatie mag door de overheid slechts worden ingezameld voor welbepaalde doeleinden en in de mate dat ze proportioneel is met deze doeleinden.

Informatie mag door het geheel van de overheidsinstellingen slechts één maal worden ingezameld, en wel zo dicht mogelijk bij de authentieke bron. De verschillende overheidsinstellingen mogen dezelfde informatie niet meermaals opvragen bij de burgers of de ondernemingen. Ook mogen zij geen informatie opvragen bij een andere bron dan waar de informatie voor het eerst gecreëerd wordt. Het komt bijvoorbeeld niet aan een werkgever toe om te bepalen of een ongeval op het werk juridisch gekwalificeerd kan worden als een arbeidsongeval; dat is de verantwoordelijkheid van de arbeidsongevallenverzekeraar. Informatie omtrent het feit of een ongeval voorgekomen op het werk al dan niet een arbeidsongeval is, moet dus worden opgevraagd bij de arbeidsongevallenverzekeraar, en niet bij de werkgever.

De informatieverstrekker moet zelf kunnen kiezen via welk kanaal hij de informatie meedeelt aan de overheid. Bij voorkeur worden elektronische kanalen gebruikt met eenvormige basisdiensten (single sign-on, ontvangstmelding per bestand, notificatie per bericht, …).

De overheidsinstellingen moeten de informatie inzamelen op basis van het informatiemodel en op basis van eenvormige administratieve richtlijnen.

Idealiter beschikt de informatieverstrekker over de mogelijkheid om de kwaliteit van de informatie te controleren alvorens ze door te geven aan een overheidsinstelling. Dit veronderstelt dat de overheid aan de informatieverstrekkers software ter beschikking stelt om de kwaliteit te controleren.

Eens de informatie bij een overheidsinstelling toekomt, moet ze volgens een vastgelegde taakverdeling eenmalig gevalideerd worden door de overheidsinstelling die daarvoor het meest competent is of die daarbij het meeste belang heeft. Slechts na deze validering mag de informatie gedeeld worden met gemachtigde gebruikers en door hen hergebruikt worden. Anders dreigt foute informatie verspreid te worden en dreigen de informatieverstrekkers door verschillende overheidsinstellingen gecontacteerd te worden met de vraag om dezelfde onjuiste informatie te verbeteren.

2.3. Beheer van informatie

Informatie in alle vormen (vb. gesproken, gedrukt, elektronisch, beelden, ...) moet doorheen haar levenscyclus op een efficiënte manier worden beheerd. Een functionele taakverdeling moet worden afgesproken omtrent welke overheidsinstelling welke informatie in authentieke vorm opslaat, beheert en toegankelijk stelt voor alle gemachtigde gebruikers. Op die manier wordt voor iedere informatie een authentieke bron vastgesteld binnen de overheid.

Informatie moet opgeslagen worden in overeenstemming met het informatiemodel en flexibel geaggregeerd kunnen worden in functie van de wijzigende wettelijke begrippen.

Elke overheidsinstelling moet vermoede onjuistheden van informatie melden aan de overheidsinstelling die ze dient te valideren. Iedere overheidsinstelling die informatie overeenkomstig de vastgelegde taakverdeling moet valideren, moet de gemelde vermoede onjuistheden analyseren, zo nodig verbeteren en de verbeterde informatie ter beschikking stellen van de gekende belanghebbende overheidsinstellingen.

Informatie mag slechts worden bewaard en beheerd zolang dat nodig is voor bedrijfsbehoeften, de ondersteuning van het beleid of de toepassing van de regelgeving, of (bij voorkeur geanonimiseerd of gecodeerd) zolang ze relevante historische of archiefwaarde heeft.

2.4. Elektronische uitwisseling van informatie

Eenmaal ingezameld en gevalideerd, moet informatie zoveel mogelijk elektronisch worden opgeslagen, beheerd en uitgewisseld om manuele heringave te vermijden. Het initiatief voor de elektronische uitwisseling van informatie kan uitgaan van de overheidinstelling die over de informatie beschikt, van de overheidsinstelling die de informatie nodig heeft of van overheidsinstellingen die elektronische informatie-uitwisseling organiseren.

De elektronische uitwisseling van informatie geschiedt best aan de hand van een functioneel en technisch operabiliteitsframework, dat geleidelijk maar permanent mee-evolueert met open marktstandaarden en onafhankelijk is van de gebruikte techniek van informatie-uitwisseling (interactief of via stapelverwerking).

De beschikbare informatie moet proactief worden gebruikt voor de automatische toekenning van rechten, de vóórinvulling bij informatie-inzameling en de informatieverstrekking aan de betrokkenen.

2.5. Informatiebeveiliging

De veiligheid, de integriteit en de vertrouwelijkheid van de informatie moet worden gewaarborgd aan de hand van een geïntegreerd geheel van structurele, organisatorische, technische, fysische en andere veiligheidsmaatregelen die uitvoering geven aan een vastgelegd informatieveiligheidsbeleid.

Persoonsgegevens mogen enkel worden gebruikt voor doeleinden die verenigbaar zijn met de doeleinden waarvoor ze zijn ingezameld. Ze mogen slechts toegankelijk zijn voor daartoe gemachtigde gebruikers in functie van de bedrijfsbehoeften, de ondersteuning van het beleid en de toepassing van de regelgeving. De toegangsmachtigingen tot persoonsgegevens worden best toegekend door een onafhankelijk, door het Parlement aangesteld comité, nadat is vastgesteld dat aan de toegangsvoorwaarden is voldaan. De toegangsmachtigingen worden openbaar gemaakt. Elke elektronische uitwisseling van persoonsgegevens wordt preventief getoetst op conformiteit met de geldende toegangsmachtigingen door een onafhankelijke instelling, die de elektronische informatie-uitwisseling organiseert. Elke elektronische uitwisseling van persoonsgegevens wordt gelogd om ieder eventueel oneigenlijk gebruik achteraf te kunnen traceren.

Telkens de informatie gebruikt wordt voor een beslissing, wordt aan de betrokkene de gebruikte informatie meegedeeld tegelijk met de mededeling van de beslissing. Elke persoon heeft recht op toegang tot en op verbetering van zijn eigen persoonsgegevens.

3. Een gebruikersgerichte re-engineering van de bedrijfsprocessen en de uitbouw van waardeketens

3.1. Algemeen

Burgers en ondernemingen zijn geïnteresseerd in een zo geïntegreerd mogelijke dienstverlening wanneer zich bepaalde gebeurtenissen voordoen. Zij willen dat processen die worden aangeboden door verschillende instanties (overheidsinstellingen, privé-bedrijven, ...) zodanig op mekaar worden afgestemd dat met een minimum aan inspanningen een maximale toegevoegde waarde wordt bekomen. Zij willen bijvoorbeeld dat bij een verhuis via één geïntegreerd proces alle administratieve formaliteiten kunnen worden afgehandeld t.a.v. de overheid in haar geheel en tegelijkertijd de gewenste diensten kunnen betrekken bij private dienstleveranciers (vb. elektriciteits- en gasmaatschappijen, verhuisfirma's, ...).

Burgers en ondernemingen wensen bovendien dat de hen aangeboden geïntegreerde diensten naadloos aansluiten op hun eigen processen. Ondernemingen willen bijvoorbeeld dat het vervullen van verplichtingen t.a.v. de overheid bij aanwerving of tewerkstelling van personeel rechtstreeks kunnen worden vervuld vanuit de eigen personeelsadministratiesoftware.

Een geïntegeerde dienstverlening die naadloos aansluit op de eigen omgeving van de burgers en de onderneming kan worden bereikt door het opbouwen van ketens van onderling verbonden processen, die we waardeketens noemen. Dit vereist een grondige re-engineering

van de bedrijfsprocessen binnen de overheid en van de dienstverleningsprocessen aan burgers en ondernemingen, en de nodige interne reorganisaties binnen de overheidsinstellingen.

De overheid kan de uitbouw van waardeketens in bepaalde domeinen coördineren, maar moet private ondernemingen en organisaties ook toelaten waardeketens uit te bouwen waarin overheidsprocessen worden geïntegreerd. Dit impliceert dat de overheid haar processen op een goed gedocumenteerde wijze aanbiedt op zodanige wijze dat ze kunnen worden ingepast in waardeketens ontwikkeld door derden.

3.2. Gevolgen voor de overheidswebsites

Overheidsinstellingen handelen alvast in strijd met een waardeketenbenadering wanneer zij elektronische diensten enkel aanbieden op eigen websites of portalen. Als elke overheidsinstelling of overheidsniveau dat doet, ontberen de burgers en ondernemingen een geïntegreerde dienstverlening. Elektronische informatie en transacties moeten door de overheidsinstellingen dus op dergelijke wijze worden aangeboden dat ze toegankelijk kunnen worden gemaakt vanop om het even welke website die een burger of onderneming wenst te gebruiken. En dit kan even goed een website zijn van andere overheidsniveaus, belangengroepen, financiële instellingen, ziekenfondsen, ... Het is strijdig met een geïntegreerde, gebruikersgerichte benadering dat overheidsinformatie en –transacties enkel op overheidswebsites worden aangeboden, en informatie en transacties die niet van de overheid afkomstig zijn enkel op niet-overheidswebsites. Concreet moet de overheid elektronische informatie m.b.t. de diensten die ze verleent en de regelgeving die ze toepast, modulair en up to date ter beschikking stelt in algemeen toegankelijke content management systemen, met gestandaardiseerde metadata, die zijn gescheiden van de inhoudelijke informatie. Wat betreft de transacties, moet de overheid componenten aanbieden die vlot kunnen worden geïntegreerd in externe websites en portalen.

Als ze eigen websites uitwerkt, moet de overheid streven naar maximale toegevoegde waarde voor de burgers en de ondernemingen. Dit kan door

- ook externe informatie en transacties ter beschikking te stellen via haar websites en portalen, zodat de gebruikers een geïntegreerde dienstverlening krijgen die maximaal tegemoet komt aan hun behoeften;
- ervoor te zorgen dat de informatie en transacties toegankelijk zijn vanuit zoveel mogelijk relevante logica's, te kiezen door de gebruiker;
- geïntegreerde work flow aan te bieden aan de gebruikers, die, indien gewenst, kan worden geïntegreerd in hun eigen work flow;
- te zorgen voor een geïntegreerd relatiebeheer met de gebruikers over de verschillende kanalen (portaal, e-mail, telefoon, ...) heen, met feedbackmechanismen voor een permanente verbetering van de dienstverlening;
- te streven naar systemen waarbij de burgers en de ondernemingen door de overheid proactief en gepersonaliseerd worden gewezen op hun rechten en verplichtingen.

3.3. De publicatie van webservices

Websites zijn bestemd voor gebruik door personen. Zoals reeds aangegeven, wensen de burgers en ondernemingen elektronische diensten aangeboden door de overheid te integreren met eigen geïnformatiseerde processen. Daartoe dient de overheid ook te voorzien in de terbeschikkingstelling van goed gedocumenteerde elektronische diensten die rechtstreeks kunnen worden aangeroepen vanuit de toepassingen van de gebruikers.

In de meeste eenvoudige vorm kunnen gestructureerde berichten worden gepubliceerd via dewelke toepassingen van gebruikers rechtstreeks kunnen communiceren met toepassingen van de overheid. Een stap verder is de publicatie van web services. Een web service is een softwarecomponent die een eenduidig zelfbeschreven functionaliteit aanbiedt en gedistribueerd aangeroepen kan worden door gebruik te maken van standaard internettechnologie. De overheid publiceert dan de door haar aangeboden web services in een repository. Geïnteresseerde gebruikers kunnen de repository raadplegen om de beschikbare diensten, de geleverde functionaliteiten en de wijze voor gebruik van de diensten te kennen, en de web services door hun toepassingen laten aanroepen.

4. Een interoperabiliteitsframework

E-government veronderstelt de mogelijkheid voor de overheidsinstellingen, hun medewerkers, de burgers en de ondernemingen om informatie te delen en bedrijfsprocessen te integreren aan de hand van een interoperabiliteitsframework. Dergelijk framework bevat minstens volgende elementen.

4.1. Technische standaarden

Heel wat internationale organisaties werken voortdurend evoluerende, open ICT-standaarden uit. De overheidsinstellingen maken best gebruik van deze standaarden als basis voor hun interoperabiliteitsframework. Doorgaans omvatten dergelijke frameworks standaarden op het vlak van

- interconnectie: netwerken (TCP/IP), mail (SMTP), directory services (LDAP), gegevenstransfer (HTTP en FTP), …
- informatie-uitwisseling: open tekst en gestructureerde gegevens (HTML en XML-schema's), beveiligde tekst (PDF), informatiemodellering (UML), informatietransformatie (XSL), web services (SOAP, UDDI), dienstenrepositories (WSDL), …
- veiligheid: transportveiligheid (SSL), veilige mail (S/MIME), digitale certificaten (X509), …

Goede voorbeelden van dergelijke, op open standaarden gebaseerde technische interoperabiliteitsframeworks zijn te vinden in het Verenigd Koninkrijk[1] en Nieuw-Zeeland[2].

4.2. Afspraken m.b.t. de functionele interoperabiliteit

Naast de technische interoperabiliteit gebaseerd op open standaarden, is er nood aan afspraken m.b.t. de functionele interoperabiliteit en de wijze waarop investeringen gedaan door deelnemers aan het interoperabiliteitsframework niet waardeloos worden telkens de technische standaarden evolueren. In dergelijke overeenkomsten moeten aspecten worden behandeld als gestandaardiseerde codes (vb. return codes, …), gestandaardiseerd gebruik van objecten en attributen, standaarden inzake de layout van de headers van berichten (onafhankelijk van het berichtformaat (EDI, XML, …) of de gebruikte methode van informatie-uitwisseling (on line, batch, …)), versiebeheer, service level agreements, beschikbaarheid van gescheiden acceptatie- en productie-omgevingen, prioriteitenbeheer, …

[1] Zie http://www.govtalk.gov.uk/
[2] Zie http://www.e-government.govt.nz/

4.3. Unieke identificatiesleutels

Informatie kan veel gemakkelijker en met hogere juistheidswaarborgen worden uitgewisseld indien alle (overheids)informatiesystemen dezelfde, unieke identificatiesleutels gebruiken voor de entiteiten waarover ze informatie dienen uit te wisselen. Uiteraard moet worden vermeden dat informatie door de overheid wordt uitgewisseld of geïnterconnecteerd zonder enige vorm van controle. Daarom hebben we hoger voorgesteld de uitwisseling en interconnectie van persoonsgegevens door de overheid afhankelijk te maken van een voorafgaandelijke machtiging van een onafhankelijk, door het Parlement benoemd orgaan.

Elke entiteit (vb. een persoon, een onderneming, een stuk grond, …) waarover informatie wordt beheerd of uitgewisseld wordt best geïdentificeerd aan de hand van eenzelfde identificatiesleutel doorheen alle (overheids)informatiesystemen. Dergelijke identificatiesleutel moet volgende kenmerken bezitten:

- uniciteit: elke entiteit heeft één en slechts één identificatiesleutel, en dezelfde identificatiesleutel is niet toegekend aan meerdere entiteiten;
- exhaustiviteit: elke entiteit die moet kunnen worden geïdentificeerd, heeft een identificatiesleutel;
- stabiliteit doorheen de tijd: de identificatiesleutel bevat geen veranderlijke kenmerken van de entiteit die hij identificeert, geen verwijzingen naar identificatiesleutels of kenmerken van andere entiteiten, en verandert niet wanneer bepaalde kenmerken veranderen van de entiteit die hij identificeert.

Bij internationale gegevensuitwisseling kan hetzij een voorvoegsel worden toegevoegd aan de nationale identificatiesleutels, of kunnen conversietabellen worden beheerd met de relatie tussen de onderscheiden nationale identificatiesleutels.

In België beschikt elke natuurlijke persoon over een uniek identificatienummer, dat hetzij wordt toegekend door het Rijksregister (voor de personen ingeschreven in een Belgisch bevolkings- of vreemdelingenregister), hetzij door de Kruispuntbank van de Sociale Zekerheid (voor de personen die een dossier hebben bij een Belgische instelling van sociale zekerheid of overheidsinstelling, maar niet (meer) ingeschreven zijn in een Belgische bevolkings- of vreemdelingenregister). Dat uniek identificatienummer wordt algemeen gebruikt als unieke identificatiesleutel door alle overheidsinstellingen. Om de uniciteit van het nummer te waarborgen, houden het Rijksregister en de Kruispuntbank van de Sociale Zekerheid m.b.t. de personen waaraan zij een nummer toekennen, een aantal basisidentificatiegegevens bij. Het betreft de naam en de voornamen, de geboortedatum en –plaats, het adres van de hoofdverblijfplaats, het geslacht, de nationaliteit en de datum en plaats van overlijden. Het Rijksregister houdt ook de gezinssamenstelling en het beroep van de betrokkene bij. Vooraleer een identificatienummer aan een natuurlijke persoon wordt toegekend, wordt eerst door raadpleging van de beschikbare gegevens nagegaan of de betrokkene niet reeds over een identificatienummer beschikt.

Het identificatienummer toegekend aan een natuurlijke persoon door de Kruispuntbank van de Sociale Zekerheid wordt vervangen door een identificatienummer toegekend door het Rijksregister zodra de betrokkene zich inschrijft in een Belgisch bevolkings- of vreemdelingenregister. In dat geval wordt echter in een conversietabel het verband bijgehouden tussen het oude en het nieuwe nummer.

De basisidentificatiegegevens opgeslagen in het Rijksregister of het register van de Kruispuntbank van de Sociale Zekerheid zijn toegankelijk voor alle overheidsinstellingen die hiertoe gemachtigd zijn door het daartoe bevoegde sectoraal comité van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Sedert 1996 beschikt elke persoon die titularis is van een uniek identificatienummer over een sociale identiteitskaart (de zgn. SIS-kaart). De SIS-kaart is een geheugenchipkaart waarop het uniek identificatienummer visueel en elektronisch leesbaar vermeld staat. Zij is geconcipieerd door de Kruispuntbank van de Sociale Zekerheid en wordt uitgereikt door de ziekenfondsen. Zij bevat naast het uniek identificatienummer ook in elektronische vorm de aanduiding van de verzekerbaarheidstoestand van de houder in de gezondheidszorg. Deze verzekerbaarheidstoestand dient gekend te zijn door bepaalde zorgverstrekkers, zoals apothekers en ziekenhuizen, om de door de patiënt te betalen kostprijs van de verstrekte zorgen juist te kunnen vaststellen. Vóór de invoering van de SIS-kaart werd de verzekerbaarheidstoestand in de gezondheidszorg bewezen met papieren kleefbriefjes, waarvan er door de apothekers en ziekenhuizen jaarlijks zowat 100 miljoen dienden te worden overgetypt. De identificatiefunctie van de SIS-kaart zal in de toekomst worden overgenomen door de elektronische identiteitskaart (zie punt 7.2.). Belangrijk is evenwel dat elke burger in België reeds sedert 5 jaar over een officiële geheugenchipkaart beschikt waarop zijn uniek identificatienummer visueel en elektronisch leesbaar vermeld staat, en die hij ter identificatie kan gebruiken in elk rechtstreeks of onrechtstreeks (vb. via zijn werkgever) met de overheid.

Ook alle ondernemingen en vestigingen van ondernemingen hebben in België sedert 1 januari 2003 een uniek identificatienummer, dat wordt toegekend door de Kruispuntbank van de Ondernemingen. Voor ondernemingen die reeds over een BTW-nummer beschikten vóór 1 januari 2003 is het ondernemingsnummer het BTW-nummer. Het begrip "onderneming" is zeer ruim, en omvat elke rechtspersoon, evenals elke natuurlijke persoon of feitelijke vereniging die een ambacht uitoefent, handel drijft, als zelfstandige een dienstverlenend, intellectueel of vrij beroep uitoefent, als werkgever aan de sociale zekerheid is onderworpen of aan de belasting op de toegevoegde waarde is onderworpen. Een natuurlijke persoon die een onderneming voert, krijgt dus naast zijn uniek identificatienummer als natuurlijk persoon ook een ondernemingsnummer dat zijn onderneming identificeert. Het ondernemingsnummer verandert niet wanneer de onderneming van eigenaar of van rechtsvorm verandert. Om de uniciteit van het ondernemingsnummer te waarborgen, houdt de Kruispuntbank van de Ondernemingen m.b.t. de ondernemingen waaraan zij een nummer toekent, een aantal basisidentificatiegegevens bij. Het betreft de naam, het adres van de maatschappelijke zetel en de vestigingen, de rechtsvorm en de rechtstoestand. Vooraleer een identificatienummer aan een onderneming persoon wordt toegekend, wordt eerst door raadpleging van de beschikbare gegevens nagegaan of de onderneming niet reeds over een identificatienummer beschikt. De basisidentificatiegegevens opgeslagen in de Kruispuntbank Ondernemingen zijn deels publiek toegankelijk. De niet-publiek toegankelijke gegevens zijn beschikbaar voor alle overheidsinstellingen die hiertoe gemachtigd zijn door het daartoe bevoegde sectoraal comité van de Commissie voor de bescherming van de persoonlijke levenssfeer.

4.4. Een gedeeld, algemeen toegankelijk informatiemodel

Zoals hoger aangegeven, moet informatie worden gemodelleerd, en worden ingezameld, beheerd en uitgewisseld overeenkomstig het model. Het model bevat typisch entiteiten, kenmerken of attributen van entiteiten en relaties tussen entiteiten, en wordt overeenkomstig de heersende standaarden best objectgeoriënteerd opgesteld. Het model wordt best beheerd in

een samenwerkingsverband tussen alle betrokkenen en is best elektronisch en openbaar toegankelijk, met een zoekmotor die een raadpleging toelaat per entiteit, versie, … Een goed versiebeheer is cruciaal, evenals de mogelijkheid om de definities van de entiteiten en de attributen uit het model te kunnen afladen in verschillende formaten.

5. Een geïntegreerd informatieveiligheidsbeleid

De uitbouw van E-government veronderstelt dat alle gebruikers terecht vertrouwen kunnen hebben in de beveiliging van de gebruikte informatiesystemen en dat de nodige maatregelen worden genomen ter bescherming van de hun persoonlijke levenssfeer. Dit veronderstelt een geïntegreerd beleid terzake over alle overheidsinstellingen heen, waarvan de bescherming van de persoonlijke levenssfeer best als een wezenlijk onderdeel wordt behandeld.

5.1. Uitgangspunten van een geïntegreerd informatieveiligheidsbeleid

De informatieveiligheid bestaat uit de preventie van schade die kan worden toegebracht aan de goede werking van de overheid en de dienstverlening aan haar gebruikers, door de aantasting van haar middelen en procedures van (elektronische) informatieverwerking. Het uiteindelijk te beschermen voorwerp, en met name de goede werking van de overheid en de persoonlijke levenssfeer van alle betrokkenen, is van uitzonderlijk belang. Gepaste maatregelen zijn dan ook nodig voor het waarborgen van de integriteit, de beschikbaarheid, de vertrouwelijkheid (o.a. finaliteits- en proportionaliteitsbeginsel), de niet-weerlegbaarheid, de authenticiteit en de auditeerbaarheid van de informatie en de informatieverwerkende systemen.
De informatisering van de overheidsinstellingen en de toenemende samenwerking inzake informatiebeheer biedt uitzicht op enorme verbeteringen op het vlak van effectiviteit en efficiëntie. Maar tegelijkertijd worden nieuwe risico's gelopen. De afzonderlijke overheidsinstellingen zijn immers niet langer op zichzelf staande informatieverwerkende eenheden, maar onderdelen van een samenhangende groep. Door de groeiende samenwerkingsverbanden wordt de kans op en omvang van gereflecteerde schade op andere systemen dan waar de basisschade zich voordoet, veel groter. De visie inzake informatieveiligheid en bescherming van de persoonlijke levensfeer dient dan ook gemeenschappelijk te worden vastgelegd. De uitvoering ervan in elke overheidsinstelling behoort tot basisverantwoordelijkheid van elke eindverantwoordelijke van een overheidsinstelling.

Het voorkomen van schade die kan worden toegebracht aan de goede werking van de informatiesystemen van de overheid enerzijds en aan de persoonlijke levenssfeer van de betrokkenen anderzijds moet op de eerste plaats komen. Preventie is namelijk de beste manier van beveiligen. Het is de actie die vermijdt dat de schade optreedt, door het tijdig opmerken en wegnemen van de bedreigingen. Primaire preventie gaat voor secundaire en tertiaire preventie, die respectievelijk de reeds aangerichte schade herstellen en verhinderen dat de opgelopen schade nog verergert. Toch zijn de 3 vormen van preventie nodig, omdat niet alle schade kan vermeden worden, ook niet bij het beste informatieveiligheidsbeleid. Bij het vastleggen van een veiligheidsbeleid is het nodig deze indeling in het oog te houden, daar ze aan het licht brengt dat sommige eenvoudige en weinig kostelijke maatregelen een groter gewicht hebben dan dure maar minder efficiënte acties.

Dit brengt ons tot een volgend veiligheidsbeginsel, namelijk dat van de risico-afweging. Elke vooruitgang en vernieuwing is het resultaat van het opzoeken van goede risico's en het vermijden

van slechte. Het wikken van de goede en de slechte risico's vergt een beredeneerde benadering: de kansen op het verwerven van winst moeten de kansen op het lijden van schade in aanzienlijke mate overtreffen. Door het opdrijven van de beveiliging kan voor een positieve balans worden gezorgd, maar ook de beveiliging brengt kosten mee die winst ernstig kunnen aantasten. De kansen op schade moeten weliswaar steeds zo klein mogelijk gehouden worden, maar tegen een redelijke prijs. De inspanningen inzake informatieveiligheid moeten dan ook gericht zijn op het bereiken van een redelijk evenwicht tussen het behalen van de winst- en het vermijden van de verlieskansen, die uit vernieuwende actie voortvloeien. Absolute veiligheid mag niet voorgesteld worden als een na te streven ideaal. Anders dreigt elke vernieuwing in de kiem te worden gesmoord.

De beveiliging van een informatiesysteem is geen technisch produkt, dat door deskundigen in het systeem kan worden ingebouwd, maar volgt uit de zorgzame uitvoering van de dagelijkse opdracht van iedere persoon die bij de werking ervan betrokken is. Wie zich een veilige toekomst wil verzekeren, moet in de eerste plaats zelf voor zijn beveiliging zorgen. Daarom is het wenselijk veiligheid op te nemen als waarde in het waardenkader van elke medewerker van de overheid, als een goed dat permanent moet worden nagestreefd.

Een deskundige kan enkel raad geven, hulpmiddelen aanwijzen, toezicht houden, motiveren, aandacht trekken, oog en oor zijn voor de gevaren waaraan de bedienaars van het te beschermen systeem zijn blootgesteld. De beveiliging zelf moet hij overlaten aan hen die het systeem bedienen. Zij en niemand anders dragen dan ook de eerste verantwoordelijkheid voor de bescherming van het systeem. De sociale organisatie van de beveiliging is daarom een conditio sine qua non van gelijk welk veiligheidssysteem. Zelfs de beste technologische hulpmiddelen kunnen nooit de sociale controle vervangen. Zij kunnen het veiligheidsniveau ongetwijfeld verbeteren, maar in laatste instantie berust veiligheid op een efficiënte organisatie.

Een informatiesysteem is zo veilig als zijn zwakste schakel. Een homogeen geheel van maatregelen is nodig, zoniet zijn de inspanningen zinloos. Daarom zijn maatregelen nodig op organisatorisch, juridisch, technisch en fysisch vlak. De veiligheidsproblematiek dient bovendien op een gestructureerde wijze aangepakt te worden en omvat in hoofdzaak de volgende fasen: de inventarisatie van de bestaande beveiligingssituatie, het vastleggen van prioriteiten in een veiligheidsbeleid, het concreet vertalen van het veiligheidsbeleid naar maatregelen vastgelegd in een veiligheidsplan, het implementeren van de geplande maatregelen, en het voortdurend toetsen of de bestaande maatregelen nog wel nodig zijn en worden nageleefd.

Het voorstellen van een omnivalente modeloplossing inzake informatieveiligheid is onmogelijk. Een onderscheid dient te worden gemaakt tussen de algemene doelstellingen, die globaal kunnen worden vastgelegd, en de manier waarop deze doelstellingen worden gerealiseerd. Bij de keuze van de manier waarop de doelstellingen worden gerealiseerd dient voldoende ruimte te worden gelaten om optimaal in te spelen op de concrete behoeften en risico's van elke omgeving. Responsabilisering van de betrokkenen via het opleggen van gecontroleerde zelfregulering werkt in dit kader efficiënter dan overnormering van bovenuit.

Veiligheid kan efficiëntie en gebruiksvriendelijkheid belemmeren en kost geld. Bovendien vernietigt de beste preventie, met name de primaire, de bewijzen van haar efficiëntie. Zij laat immers de schade niet ontstaan. Dit veroorzaakt mettertijd een valse indruk van nutteloosheid, gevolgd door verslapping van de aandacht en van de inspanning. Daarom is een volgehouden motivatie en sensibilisatie, en de permanente investering in informatieveiligheid onontbeerlijk. Tegen het bijna wetmatig verval van de preventieve inspanning moet permanent en zeer bewust

worden ingegaan. Dit vergt een voortdurende opvijzeling van de veiligheidsmoraal, zowel bij het kaderpersoneel als bij hun ondergeschikten. Misschien is dit wel een van de moeilijkste taken.

Het informatieveiligheidsbeleid moet tenslotte conform zijn aan de geldende regelgeving, o.a. inzake de bescherming van de persoonlijke levenssfeer of de elektronische handtekening.

5.2. De verdere uitbouw overeenkomstig de ISO-norm 17799

De verdere vormgeving van de informatieveiligheid geschiedt best op basis van internationaal aanvaarde ISO-normen; in casu zijn vooral de ISO-norm 17799 (Code of practice inzake informatieveiligheid) en ISO-norm 15408 (Evaluatiecriteria voor ICT-veiligheid) van groot belang. De ISO-norm 17799 bevat 10 hoofddomeinen van beveiliging, waarvoor telkens een checklist van concrete maatregelen is opgesteld. Het betreft de organisatie, het veiligheidsbeleid, de classificatie van informatie, de beveiligingseisen t.a.v. personeel, de fysieke beveiliging van de omgeving, het beheer van communicatie- en bedieningsprocessen, de toegangsbeveiliging, de ontwikkeling en onderhoud van systemen, het continuïteitsmanagement en de interne en externe controle op de naleving. Inzake E-government worden deze hoofddomeinen best aangevuld met bijzondere maatregelen inzake de verwerking van persoonsgegevens en de externe communicatie inzake het informatieveiligheidsbeleid. De maatregelen inzake beleid, organisatie, beveiligingseisen t.a.v. personeel en classificatie vormen de bouwstenen om de informatieveiligheid van de grond te krijgen. Ze zijn dan ook prioritair. Voor de andere domeinen noemt de ISO-norm 17799 3 bronnen voor het vaststellen van prioriteiten:

- de inschatting van de grootste risico's;
- de externe conformiteitsanalyse, met name de conformiteit met datgene wat wordt voorgeschreven door de wet of de contracten en wat goed gebruik is in de sector;
- de interne conformiteitsanalyse, met name de gevolgen voor de informatiesystemen en hun veiligheid die voortvloeien uit de evoluerende bedrijfsdoelstellingen (vb. een overheidsportaal moet 24/7 beschikbaar zijn aan goede performantie).

Om prioriteiten te stellen, wordt aangeraden een baseline-toets door te voeren. Dit houdt in dat per informatiesysteem wordt nagegaan of een aantal baseline-maatregelen voldoende worden geacht als beveiligingsmaatregelen in functie van de 3 vermelde bronnen. Enkel indien deze baseline-maatregelen niet voldoende lijken, wordt voorgesteld een gedetailleerde risico-analyse uit te voeren. Bij het uitvoeren van de risico-analyse voor de informatiesystemen waarvoor de baseline-maatregelen niet volstaan, moeten de 2 risico-aspecten, de mogelijke schade door een incident en de waarschijnlijkheid van een incident, worden afgezet tegen de kost van de maatregelen om het risico te vermijden.

6. Een aangepast juridisch kader

6.1. Wettelijke vastlegging van de principes betreffende de omgang met informatie door de overheid

Opdat de principes die in punt 2. zijn voorgesteld, afdwingbaar zouden zijn voor de burgers en ondernemingen en tussen overheidsinstellingen, worden ze best wettelijk verankerd.

Sommige van deze principes, zoals het beginsel dat informatie door overheidsinstellingen slechts kan worden ingezameld voor welbepaalde doeleinden en op een wijze die proportioneel is aan deze doeleinden en het merendeel van de principes met betrekking tot de

bescherming van informatie, zijn vermeld in de Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Deze principes zijn dus reeds geïntegreerd in de regelgeving inzake gegevensbescherming.

Bepaalde andere principes zijn wettelijk verankerd in de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid[3] en in artikel 102 van de Programmawet van 30 december 2001[4].

Deze wetten voorzien, respectievelijk voor de sociale sector en de federale overheid, in een wettelijke basis om

- een functionele taakverdeling vast te leggen tussen (overheids)instellingen op het vlak van validatie, opslag en beheer van informatie;
- (overheids)instellingen te verplichten om de informatie die ze nodig hebben elektronisch in te zamelen bij andere (overheids)instellingen, voor zover deze informatie reeds beschikbaar is bij één van deze (overheids)instellingen;
- (overheids)instellingen te verplichten de informatie die ze beheren elektronisch mee te delen aan andere overheidsinstellingen die de informatie nodig hebben voor de uitvoering van hun opdrachten;
- het gebruik van unieke identificatienummers mogelijk te maken of op te leggen;
- de modaliteiten van de inzameling en de uitwisseling van informatie te bepalen;
- specifieke wetten, die de modaliteiten van de inzameling, de uitwisseling of het beheer van informatie beschrijven aan te passen om ze met de principes in overeenstemming te brengen.

De eerstgenoemde wet heeft tevens de verplichting ingevoerd om voor elke mededeling van persoonsgegevens door een instelling van sociale zekerheid vooraf een machtiging te bekomen vanwege een onafhankelijk, door het Parlement aangeduid comité. De Kruispuntbank van de Sociale Zekerheid gaat vóór elke mededeling van persoonsgegevens door een instelling van sociale zekerheid na of de mededeling wel in overeenstemming is met de betrokken machtiging. De Kruispuntbank van de Sociale Zekerheid heeft daarenboven een wettelijke verplichting om het noodzakelijk functioneel en technisch operabiliteitsframework te ontwikkelen. Op basis van dit model worden nu ook in andere overheidssectoren onafhankelijke comités met gelijkaardige opdrachten worden geïnstalleerd. Om de noodzakelijke coördinatie en coherentie te garanderen, zijn al deze comités opgericht als sectorale comités van de Commissie voor de bescherming van de persoonlijke levenssfeer. Elk sectoraal comité zal worden voorgezeten door een lid van de Commissie voor de bescherming van de persoonlijke levenssfeer en zal zijn samengesteld uit leden van deze Commissie en uit door het Parlement aangeduide, onafhankelijke deskundigen uit de betrokken sector.

6.2. Coherente begrippenapparaten

Juristen worden er tijdens hun opleiding op gewezen dat elke regelgevende tekst dient te steunen op duidelijke definities van de begrippen die verder in de reglementering worden

[3] Belgisch Staatsblad van 22 februari 1990. Een gecoördineerde versie van deze wet is terug te vinden op http://www.ksz.fgov.be, onder de rubriek "wetgeving".

[4] Belgisch Staatsblad van 31 december 2001.

gehanteerd. Regelmatig worden dezelfde begrippen in verschillende regelgevingen echter verschillend gedefinieerd.

Overheidsinstellingen die bij burgers of ondernemingen informatie opvragen hebben nogal eens de neiging om de juridische kwalificatie van de feitelijke realiteit in functie van de in de regelgeving gedefinieerde begrippen door te schuiven naar de informatieverstrekker. Deze moet daartoe dan vaak omvangrijke instructies doorploegen en trachten te begrijpen. Regelmatig moet hij zelfs dezelfde werkelijkheid interpreteren in functie van verschillende regelgevingen die een verschillende invulling geven aan dezelfde begrippen.

Dit euvel kan worden vermeden door tijdens het regelgevend proces enkele duidelijke principes toe te passen. Definities in de regelgeving mogen nog steeds verschillen, maar zouden nog uitsluitend mogen verwijzen naar dezelfde informatie-elementen en -kenmerken die tijdens het voorgestelde proces van informatiemodellering werden bepaald. Juristen kunnen aldus zoveel definities redigeren als ze zelf willen, maar die definities moeten wel zijn opgebouwd uit verwijzingen naar dezelfde informatie-elementen en –kenmerken, die in het informatiemodel werden vastgelegd. Indien een noodzakelijk informatie-element nog niet werd gedefinieerd binnen het informatiemodel, moet dat gebeuren maar op een wijze die verenigbaar is met de hogergenoemde principes inzake informatiemodellering.

Door deze aanpak moeten burgers en ondernemingen niet langer zelf overgaan tot het interpreteren van dezelfde werkelijkheid in functie van uiteenlopende wettelijke definities. Ze moeten enkel nog informatie verschaffen die overeenstemt met het informatiemodel. De diverse overheidsinstellingen kunnen deze informatie dan gebruiken om hun respectieve taken uit te voeren.

Het weze duidelijk dat het volgen van deze principes een grote discipline vergt van eenieder die betrokken is bij het opstellen van regelgevende teksten. Bovendien moet er een grondig gedocumenteerd informatiemodel beschikbaar zijn. De Raad van State is belast om de kwaliteit van regelgeving te onderzoeken vooraleer ze wordt uitgevaardigd. Ze zou een belangrijke rol kunnen vervullen bij het implementeren van de voorgestelde principes.

De hiervoor beschreven visie werd met succes toegepast binnen de Belgische sociale zekerheid voor bepaalde begrippen (“woonplaats”, “loon”, “arbeidsdag”, “gelijkgestelde dag”, “referteperiode”,…) die voorheen heel uiteenlopend werden gedefinieerd doorheen de verschillende takken van de sociale zekerheid. De daarbij gehanteerde methodologie werd beschreven in de paper “E-government: the approach of the Belgian federal administration”, die kan worden gedownload van de website van de auteur van deze bijdrage[5].

6.3. Aangepaste ICT-regelgeving

E-government en, in het algemeen, de trend tot ruim gebruik van ICT vereist een afdoende reglementering van aspecten zoals de bescherming van grondrechten bij de verwerking van persoonsgegevens, bescherming tegen ICT-misdrijven, ICT-beveiliging, bewijskracht van elektronische informatie, elektronische handtekeningen, gelijke toegang tot openbare diensten, openbaarheid van bestuur,… In een geglobaliseerde wereld, waar veel processen niet beperkt blijven binnen de eigen landsgrenzen, moeten veel van die regels op

[5] Zie http://www.law.kuleuven.ac.be/icri/frobben, rubriek “Presentaties”.

internationaal vlak gecoördineerd worden. Elk land heeft dan de verplichting om de internationaal uitgewerkte principes in zijn eigen wetgeving te integreren.

De Europese Unie is heel bedrijvig geweest in het uitwerken van gecoördineerde regels op een aantal hogervermelde domeinen. Dit werd over het algemeen gerealiseerd door middel van richtlijnen, waarvan o.a. de volgende in dit kader relevant zijn

- Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[6];
- Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector[7];
- Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen[8];
- Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (richtlijn inzake elektronische handel)[9];
- Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)[10].

In de domeinen waar Europese richtlijnen werden uitgevaardigd, nam België de gewoonte aan om de richtlijnen om te zetten in nationale wetgeving waarvan de tekst heel nauw aansluit bij die van de richtlijn zelf. Dit was onder meer het geval met

- de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens[11], grotendeels gewijzigd bij de wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG[12], en het koninklijk besluit van 13 februari 2001 tot uitvoering van de wet van 8 december 1992[13];
- de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en -telecommunicatie[14];
- de wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure[15];
- de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten[16].

In de domeinen waar geen Europese richtlijnen werden uitgevaardigd, heeft België zijn eigen regelgeving gecreëerd. Dit was bijvoorbeeld het geval met de wet van 11 april 1994

---

6 Publicatieblad nr. L 281 van 23 november 1995, p. 31.
7 Publicatieblad nr. L 24 van 30 januari 1998, p. 1.
8 Publicatieblad nr. L 13 van 19 januari 2000, p. 12.
9 Publicatieblad nr. L 178 van 17 juli 2000, p. 1.
10 Publicatieblad nr. L 201 van 31 juli 2002, p. 37.
11 Belgisch Staatsblad van 18 maart 1993, p. 5801.
12 Belgisch Staatsblad van 3 februari 1999, p. 3049.
13 Belgisch Staatsblad van 13 maart 2001, p. 7839.
14 Belgisch Staatsblad van 24 januari 1995, p. 1542.
15 Belgisch Staatsblad van 22 december 2000, p. 42968.
16 Belgisch Staatsblad van 29 september 2001, p. 33070.

betreffende de openbaarheid van bestuur[17] en de wet van 28 november 2000 inzake informaticacriminaliteit[18].

Over het algemeen kan men zeggen dat de Belgische ICT-regelgeving voldoende uitgebreid en ontwikkeld is om E-government op een rechtszekere wijze mogelijk te maken.

7. Twee internationaal erkende Belgische best practices inzake E-government

7.1. De procesherziening in de sociale sector

De Belgische sociale zekerheid bestaat enerzijds uit 3 verzekeringsstelsels (werknemers, zelfstandigen en ambtenaren), waarbij maximum 7 sociale risico's (arbeidsongeschiktheid, arbeidsongeval, beroepziekte, werkloosheid, ouderdom, kinderlast en jaarlijkse vakantie – de zgn. takken van de sociale zekerheid) gedekt zijn, en anderzijds uit 4 bijstandsstelsel (tegemoetkomingen aan gehandicapten, gewaarborgde gezinsbijslag, leefloon en inkomensgarantie voor bejaarden), waarbij aan mensen bepaalde minimumvoorzieningen worden toegekend na een bestaansmiddelentoets. In het totaal zijn zowat 2.000 actoren in de sociale sector belast met de uitvoering van de Belgische sociale zekerheid. Meer dan 10.000.000 sociaal verzekerden en 220.000 werkgevers treden zeer regelmatig in contact met deze actoren om hun rechten te laten gelden, hiertoe informatie te verstrekken of bijdragen te betalen.

Uit een grondige analyse van de werking van de sociale zekerheid is destijds gebleken dat:

- de business processen van de actoren in de sociale sector weinig gebruikersgericht georganiseerd waren en zeker over actoren in de sociale sector heen niet op mekaar afgestemd;
- elke actor in de sociale sector zijn eigen set van papieren formulieren met bijhorende instructies had, aan de hand waarvan, bij het zich voordoen van een sociaal risico, de informatie werd opgevraagd die specifiek nodig was om de rechten toe te kennen naar aanleiding van dat concreet risico;
- de actoren in de sociale sector aan de sociaal verzekerden en hun werkgevers zeer vaak vroegen om reeds bij een andere actor in de sociale sector beschikbare informatie aldaar in de vorm van een papieren attest op te vragen en dat attest in te leveren, eerder dan de informatie rechtstreeks bij elkaar op te halen;
- de sociaal verzekerden en hun werkgevers aldus eenzelfde realiteit moesten meedelen aan tal van actoren in de sociale sector, telkens overeenkomstig andere juridische begrippen en administratieve instructies;
- sociaal verzekerden en hun werkgevers zelf doorheen het systeem van de sociale zekerheid hun rechten moesten opeisen, en niet konden rekenen op de automatische toekenning van alle rechten aan de hand van één aangifte.

Met de hogervermelde principes inzake het gebruik van informatie als strategische productiefactor het achterhoofd is daarom een globale herdenking van de processen doorheen de hele sociale zekerheid voor werknemers en ambtenaren doorgevoerd, volgens een duidelijk stappenplan:

[17] Belgisch Staatsblad van 30 juni 1994, p. 17662.
[18] Belgisch Staatsblad van 3 februari 2001, p. 2909.

- de integratie van het uniek identificatienummer van elke sociale verzekerde in de gegevensbanken van alle actoren in de sociale sector;
- de openstelling van bestaande gegevensbanken voor alle actoren in de sociale sector;
- de geleidelijke vervanging van bestaande papieren attesten afgeleverd door één actor in de sociale sector en bestemd voor een andere actor in de sociale sector door elektronische gegevensstromen;
- de ontwikkeling van elektronische gegevensstromen tussen actoren in de sociale sector gebaseerd op een re-engineering en betere onderlinge afstemming van bedrijfsprocessen en begrippenapparaten;
- de ontwikkeling van elektronische gegevensstromen tussen actoren in de sociale sector enerzijds en sociale verzekerden en hun werkgevers anderzijds.

Dit heeft geleid tot volgende situatie:

- de sociaal verzekerde en zijn werkgever moet nog slechts in volgende gevallen een aangifte doen aan de sociale zekerheid in zijn geheel
  - uiterlijk bij het begin van een arbeidsrelatie moet de werkgever aangeven op welk tijdstip (datum en uur) de betrokken werknemer in dienst treedt;
  - driemaandelijks moet de werkgever aangeven welk loon elk van zijn werknemers verdiend heeft, ingedeeld in looncomponenten die voortaan uniform zijn gedefinieerd doorheen alle takken van de sociale zekerheid voor werknemers en ambtenaren, en hoeveel arbeidsdagen en hiermee gelijkgestelde dagen elk van zijn werknemers gepresteerd heeft, ingedeeld in soorten dagen die voortaan ook uniform zijn gedefinieerd doorheen alle takken van de sociale zekerheid voor werknemers en ambtenaren;
  - bij het zich voordoen van een sociaal risico moet de sociaal verzekerde of zijn werkgever enkel de informatie aangeven m.b.t. dat sociaal risico; informatie m.b.t. het historisch loon of de historische arbeids- of hiermee gelijkgestelde prestaties moet niet meer worden meegedeeld, want wordt gehaald uit de driemaandelijkse aangifte van de loon- en arbeidstijdgegevens; enkel indien loon- en arbeidstijdgegevens nodig zijn m.b.t. een periode waarvoor de driemaandelijkse aangifte nog niet is verricht, moeten voor die periode nog de loon- en arbeidstijdgegevens worden meegedeeld, in de vorm van een voorlopige aangifte en overeenkomstig exact dezelfde principes als de driemaandelijkse aangifte;
  - uiterlijk bij het einde van een arbeidsrelatie moet de werkgever aangeven op welk tijdstip (datum en uur) de betrokken werknemer uit dienst treedt;
- alle aangiften van het begin en het einde van een arbeidsrelatie moeten elektronisch gebeuren, hetzij via de uitwisseling van XML-berichten tussen toepassingen, hetzij via transacties beschikbaar op het portaal van de sociale zekerheid, hetzij via een vocale server; de aangiften kunnen elektronisch gewijzigd worden via dezelfde kanalen; elke werkgever heeft via transacties op het portaal van de sociale zekerheid toegang tot de lijst van zijn werknemers, en kan via file transfer in XML-formaat een elektronische lijst van zijn werknemers bekomen, zodat hij geen eigen personeelsregister meer moet bijhouden;
- alle driemaandelijkse aangiften van loon- en arbeidstijdgegevens moeten elektronisch gebeuren, hetzij via de uitwisseling van XML-berichten tussen toepassingen, hetzij via transacties op het portaal van de sociale zekerheid; de aangiften kunnen elektronisch gewijzigd worden via dezelfde kanalen;
- alle aangiften van sociale risico's kunnen op papier of elektronisch gebeuren, hetzij via de uitwisseling van XML-berichten tussen toepassingen, hetzij via transacties beschikbaar op het portaal van de sociale zekerheid;

- de elementen vervat in de XML-schema's zijn uniform gedefinieerd over alle aangiften heen; de XML-schema's per aangifte kunnen gedownload worden vanop het portaal van de sociale zekerheid; elke 3 maanden is een nieuwe versie van de XML-schema's beschikbaar met de aanduiding van de wijzigingen t.o.v. de vorige versie, die rekening houdt met de aanpassingen van de regelgeving;
- alle actoren in de sociale sector zijn aangesloten op een netwerk voor elektronisch gegevensverkeer beheerd door de Kruispuntbank van de Sociale Zekerheid en hebben de wettelijke verplichting alle informatie die in het netwerk beschikbaar is elektronisch bij mekaar op te vragen;
- de Kruispuntbank van de Sociale Zekerheid beheert een verwijzingsrepertorium, dat aangeeft
  - voor elke burger, bij welke actoren in de sociale sector hij gekend is, in welke hoedanigheid en over welke periode;
  - per soort actor in de sociale sector en hoedanigheid waarin een sociaal verzekerde bij deze actor gekend kan zijn, welke soorten gegevens over de sociaal verzekerde beschikbaar zijn;
  - per soort actor in de sociale sector en hoedanigheid waarin een sociaal verzekerde bij deze actor gekend kan zijn, welke soorten gegevens deze actor nodig heeft en gemachtigd is om te verkrijgen om haar taken te vervullen;
- de Kruispuntbank van de Sociale Zekerheid gebruikt dat verwijzingsrepertorium om
  - er preventief over te waken dat een actor in de sociale sector enkel toegang krijgt tot de gegevens waartoe hij toegang mag hebben en over de personen die bij haar gekend zijn;
  - vragen om gegevens te routeren naar de actor in de sociale sector die de betrokken gegevens kan aanleveren;
  - gegevens die haar worden meegedeeld automatisch over te maken aan de actoren in de sociale sector die de betrokken gegevens kunnen gebruiken om hun taken te vervullen.

De resultaten mogen worden gezien:
- zowat 170 soorten papieren attesten die een sociaal verzekerde of zijn werkgever bij één actor in de sociale sector moest opvragen om ze bij een andere actor in de sociale sector af te geven, zijn afgeschaft en vervangen door rechtstreekse elektronische gegevensuitwisselingen tussen de betrokken actoren; in 2003 werden tussen de 2.000 actoren in de sociale sector 339 miljoen elektronische berichten uitgewisseld, met een end-to-end-responstijd voor on-line-gegevensuitwisselingen van minder dan 4 seconden in 99,2 % van de gevallen;
- zowat 50 soorten aangifteformulieren t.a.v. de sociale zekerheid zijn afgeschaft;
- de 30 resterende aangifteformulieren t.a.v. de sociale zekerheid zijn gemiddeld herleid tot één derde van het aantal rubrieken;
- inmiddels kunnen ondernemingen of hun vertegenwoordigers, zoals de sociale secretariaten, 23 elektronische transacties uitvoeren; op korte termijn wordt ook ten behoeve van de sociaal verzekerden voorzien in de eerste transacties via het portaal van de sociale zekerheid;
- heel wat aangiften worden rechtstreeks elektronisch gedaan vanuit de personeelsadministratie- en boekhoudingspakketten bij de werkgevers;
- sociaal verzekerden en hun werkgevers kunnen voortaan alle aangiften aan de sociale zekerheid verrichten aan de hand van een uniform begrippenapparaat en uniforme instructies, en moeten elk gegeven nog maar eenmalig meedelen aan de sociale zekerheid in zijn geheel;

- het aantal administratieve contacten van sociaal verzekerden en hun werkgevers met de sociale zekerheid is drastisch verminderd;
- de overblijvende contacten worden gestroomlijnd volgens evenementen uit het leven van de sociaal verzekerden of in de arbeidsrelatie tussen werkgever en werknemer/ambtenaar (in dienst treden, arbeid presteren, ziek worden, uit dienst treden, werkloos worden, gepensioneerd worden, ...);
- een persoonlijke dienstverlening aan de werkgevers en de sociaal verzekerden wordt aangeboden;
- een heel aantal afgeleide rechten worden automatisch toegekend zonder dat de sociaal verzekerden of hun werkgevers nog aanvragen moeten doen; zo verwerven werklozen en personen in arbeidsongeschiktheid automatisch hun pensioen op de vereiste leeftijd zonder een aanvraag te moeten indienen via de gemeente, of krijgen bepaalde sociaal zwakkere categorieën (rechthebbenden op een leefloon of op tegemoetkomingen aan gehandicapten, ...) automatisch verminderingen op bijdragen, heffingen of belastingen, een sociaal telefoontarief of een gratis abonnement voor het openbaar vervoer.

7.2. De elektronische identiteitskaart

Met de elektronische identiteitskaart heeft België een middel uitgebouwd dat gebruikers van overheidsinstellingen toelaat om zich elektronisch te identificeren en te authentiseren, en een gekwalificeerde elektronische handtekening te plaatsen in de zin van de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen[19]. De elektronische identiteitskaart is dan ook een belangrijk middel voor een efficiënt E-government, dat echter ook kan worden gebruikt in relaties tussen burgers en/of ondernemingen onderling.

7.2.1. Toelichting bij een aantal begrippen

Een PKI (afkorting van Public Key Infrastructure) is een systeem dat aan gebruikers van elektronische communicatiediensten digitale sleutelparen (telkens bestaande uit een private sleutel en een publieke sleutel) ter beschikking stelt, aan de hand waarvan zij hun elektronische communicatie kunnen beveiligen en authentiseren (d.w.z. waarborgen dat de communicatie van een bepaalde bron afkomstig is en niet gewijzigd is t.o.v. het moment van verzending door deze bron).

De beveiliging en authentisering via het gebruik van digitale sleutelparen is gebaseerd op het principe van de asymmetrische vercijfering: wat vercijferd wordt met de private sleutel, kan enkel worden ontcijferd met de bijhorende publieke sleutel, en omgekeerd. De private sleutel van een sleutelpaar mag enkel kunnen worden gebruikt door de titularis van het sleutelpaar en moet dus op een veilige wijze worden bewaard. De publieke sleutel van het sleutelpaar moet kunnen worden gebruikt door elk potentieel contactpersoon van de titularis van de private sleutel, en dus publiek toegankelijk zijn in een gegevensbank.

Indien de sleutelparen worden gebruikt om elektronische communicatie te authentiseren (d.w.z. te waarborgen dat de communicatie van een bepaalde bron afkomstig is en niet gewijzigd is t.o.v. het moment van verzending door deze bron), worden ze eenduidig verbonden aan één of meerdere certificaten, waarin de identiteit en/of één of meerdere kenmerken van deze bron staan vermeld.

[19] Publicatieblad nr. L 13 van 19 januari 2000, p. 12.

Digitale sleutelparen die door een PKI-infrastructuur ter beschikking worden gesteld, kunnen voor verschillende doeleinden worden gebruikt, zoals encryptie van berichten (om de vertrouwelijkheid en integriteit te waarborgen), authentisering bij het raadplegen van websites, het plaatsen van gekwalificeerde elektronische handtekeningen met juridische waarde,… Algemeen wordt er om veiligheidsredenen echter voor gepleit dat het sleutelpaar dat wordt gebruikt voor het plaatsen van een elektronische handtekening met juridische waarde, niet ook gebruikt wordt voor authentisering bij de toegang tot websites of voor encryptie.

Bij het uitreiken van certificaten, kunnen 2 rollen worden onderscheiden:

- de rol van registratie-autoriteit (RA): de RA is het 'loket' waar het certificaat wordt aangevraagd; ze gaat na of de opgegeven identiteit of het opgegeven kenmerk juist is; indien dit het geval is, keurt ze de aanvraag goed, en informeert hierover de certificatie-autoriteit;
- de certificatie-autoriteit (CA): de CA produceert op basis van de informatie die ze van de RA heeft verkregen een certificaat, dat ze verbindt met een sleutelpaar en dat aangeeft wat dat sleutelpaar voortaan bewijst.

Daarnaast is er ook nog de rol van directory service (DS), die zorg draagt voor het publiceren van de certificaten die door een certificatie-autoriteit zijn uitgegeven, en eventueel de inhoud van deze certificaten. De status van een certificaat kan worden nagegaan d.m.v. een OCSP (Online Certificate Status Protocol) responder die onmiddellijk antwoordt of het certificaat nog geldig is of niet.

Een elektronische handtekening is een juridisch geldig alternatief voor een handgeschreven handtekening. De Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen verplicht de Lidstaten tot het aanpassen van hun wetgeving om onder bepaalde voorwaarden rechtskracht te geven aan elektronische handtekeningen. De actueel meest gebruikte techniek voor het genereren van een elektronische handtekening is de techniek van de digitale sleutelparen met bijhorend certificaat.

Een certificaat kan de identiteit bewijzen van de sleutelpaarhouder en/of één of meerdere van diens kenmerken, zoals hoedanigheden (vb. gediplomeerde arts), functies (bv. voorzitter van de Federale Overheidsdienst Justitie) of mandaten (bv. het recht om financiële verrichtingen te doen tot een bepaald bedrag),... Een handgeschreven handtekening bewijst enkel de identiteit van een persoon, niet diens kenmerken. Kenmerken worden immers met andere middelen bewezen (bv. de vermelding van een functie onder de handtekening). Om een persoon toe te laten met hetzelfde sleutelpaar en bijhorend certificaat een juridisch geldige elektronische handtekening te plaatsen ongeacht een hoedanigheid of een functie, bevat dergelijk certificaat best alleen informatie over de identiteit van de sleutelpaarhouder, en geen informatie over diens kenmerken. Het opnemen van informatie over kenmerken in een certificaat dat is verbonden met een sleutelpaar dat wordt gebruikt voor het plaatsen van een juridisch geldige elektronische handtekening is suboptimaal omdat het het een veralgemeend gebruik van die elektronische handtekening beperkt.

7.2.2. De elektronische identiteitskaart

De Belgische elektronische identiteitskaart heeft de volgende functies:

- het visueel en elektronisch identificeren van de houder;
- het elektronisch authentiseren van de houder door middel van de techniek van de digitale handtekening;
- het genereren van een gekwalificeerde elektronische handtekening door middel van de techniek van de digitale handtekening (niet-verwerping);
- eventueel later, het bewijzen van de karakteristieken van de houder door middel van de techniek van de digitale handtekening, op initiatief van de houder.

De Belgische elektronische identiteitskaart heeft dus bijvoorbeeld niet de functie van elektronisch betaalmiddel.

De Belgische elektronische identiteitskaart neemt de vorm aan van een processorchipkaart. Enerzijds worden gegevens gedrukt op de kaart, anderzijds worden gegevens opgeslagen in de processorchip van de kaart. Volgende gegevens worden gedrukt op de kaart, en zijn dus visueel leesbaar: de unieke identificatiesleutel van de houder (dat is zijn rijksregisternummer), het kaartnummer, de basisidentificatiegegevens van de houder (naam, voornamen, geslacht, geboortedatum en -plaats), een foto van de houder, de geldigheidsperiode van de kaart. Dezelfde gegevens zijn ook opgenomen in de processorchip van de kaart, en zijn dus ook elektronisch leesbaar. Daarenboven bevat zijn ook nog opgeslagen in de processorchip van de kaart: het adres van de houder, een private sleutel met bijhorend identiteitscertificaat bruikbaar voor elektronische authentisering van de houder en een private sleutel met bijhorend identiteitscertificaat bruikbaar voor het plaatsen van de gekwalificeerde elektronische handtekening door de houder.

Het gebruik van de private sleutels en de bijhorende identiteitscertificaten wordt beveiligd met een PIN-code. Voor het plaatsen van een gekwalificeerde elektronische handtekening moet de PIN-code worden ingegeven telkens een handtekening wordt geplaatst. Voor de authentisering en het plaatsen van een elektronische handtekening wordt dus geen beroep gedaan op de verificatie van biometrische eigenschappen (bv. digitale vingerafdruk, stemherkenning,…). Het gebruik van biometrie wordt nog niet haalbaar geacht op een dergelijk ruime schaal, o.a. omwille van de nood aan ingewikkelde en dure randapparatuur.

In de processorchip van de elektronische identiteitskaart worden geen andere gegevens worden opgeslagen dan de hogervermelde. Er is immers duidelijk voor gekozen om de kaart enkel te gebruiken als middel voor identificatie, authentisering en het plaatsen van een gekwalificeerde elektronische handtekening, en niet als transportmiddel voor gegevens. Het is een bewuste optie om gegevens te transporteren via netwerken, met de kaart als identificatie- en authoriseringsmiddel om toegang te verstrekken tot gegevens m.b.t. de houder van de kaart. De opslag van gegevens op de kaart impliceert immers dat de houder deze gegevens moet updaten telkens ze wijzigen. De elektronische gegevensuitwisseling via een netwerk ontlast de houder van de kaart van de regelmatige updating van de kaart en biedt voor de gebruiker van de gegevens meer waarborgen inzake beschikbaarheid en kwaliteit van de gegevens.

De overheid heeft op basis van een offerte-aanvraag enerzijds een dienstverlener gekozen voor de aanmaak van de elektronische identiteitskaart, en anderzijds een certificatie-autoriteit gekozen voor het aanmaken van de identiteitscertificaten. De gemeenten treden op als registratieautoriteit voor de toekenning van de identiteitscertificaten; in de praktijk wil dit zeggen dat de gemeente als loket fungeert t.a.v. de houder van een elektronische

identiteitskaart en de controle van de identiteit voor de aflevering van de identiteitskaart ook gebruikt wordt als registratie voor de aflevering van de identiteitscertificaten.

Opdat de elektronische identiteitskaart in de zin van de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen als veilig middel zou kunnen worden beschouwd voor het plaatsen van een gekwalificeerde elektronische handtekening, zal ze op conformiteit met de vereisten vastgelegd in bijlage III van deze Richtlijn worden getoetst door een daartoe bevoegd orgaan. Bovendien wordt van de door de overheid gekozen certificatie-autoriteit vereist dat zij zich laat accrediteren door een daartoe bevoegd orgaan, waarbij wordt nagegaan of zijzelf en de door haar afgeleverde certificaten voldoen aan de bijlagen I en II van de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen. Om aan de gebruikers van de elektronische identiteitskaart tenslotte waarborgen te kunnen geven omtrent de goede werking van leesapparaten en bijhorende software van de elektronische identiteitskaart, wordt bij koninklijk besluit een registratieprocedure van de apparaten en de bijhorende software uitgevaardigd. Deze procedure zal worden gecombineerd met de reeds bestaande registratieprocedure voor de leesapparaten en bijhorende software van de SIS-kaart[20].

[20] Deze procedure wordt toegelicht op www.ksz.fgov.be, in de rubriek “SIS-kaart”, trefwoord “leesapparatuur van de SIS-kaart”.