E-government: the approach of the Belgian federal administration

Jan Deprest
President
FEDICT

Frank Robben
General manager
Crossroads Bank for Social Security
Strategic advisor
FEDICT

Brussels, June 2003

Table of contents

List of figures

About the authors

17 years ago, Frank Robben wrote a study on how the Belgian social security administration could be rationalized through the strategic use of ICT[1]. The study was awarded a scientific prize. After he had graduated in law and had had some additional training in ICT, he was appointed at the age of 24 strategic advisor to the Minister of Social Affairs. His mission was to implement the ideas put forward in the study in the social security sector.

Today the automation of the Belgian social security system is mentioned as a best practice in the most recent web-based survey on electronic public services ordered by the European Commission[2]. This is the result of a long-term effort, started 12 years ago, of all Belgian social security offices. This effort was co-ordinated by the Crossroads Bank for Social Security (CBSS)[3], a semi-governmental body specifically created in 1991 to stimulate the automation process, which Frank was asked to found and manage.

During this period he also had the opportunity to collaborate with successive Belgian governments on E-government initiatives in other sectors. This resulted in an ambitious plan that is being executed nowadays by the recently created Federal Public Service for Information and Communication Technology (FEDICT)[4]. During a certain period Frank combined the general management of the Crossroads Bank for Social Security with the chairmanship of FEDICT, but he put the latter mandate at the disposal of the Government because a combination of both functions had become unworkable.

The Government then appointed Jan Deprest as president of the Federal Public Service for Information and Communication Technology. Before that, Jan worked during a long period as a consultant and partner in a multinational consultancy company and then as managing director of an ICT service company responsible for the automation of the Flemish public administration. He gained a large experience in managing E-government programs. Moreover, he has an extended network of contacts in the financial and ICT sectors, on which he can rely to develop an optimal collaboration between the administration and those sectors for the extension of E-government.

By writing this paper, Frank, who is still working for FEDICT as a strategic advisor, and Jan want to share their vision and experience regarding E-government with you, and invite you to comment.

You can get in touch with Frank Robben and Jan Deprest at:

frank.robben@bcss.fgov.be
jan.deprest@fedict.be

[1] VIAENE, J., ROBBEN, F, LAHAYE, D. and VAN STEENBERGE, J., "Ebauche générale d'un traitement rationnel de l'information en sécurité sociale", Revue belge de sécurité sociale, 1986, 389-462.
[2] See http://europa.eu.int/information_society/eeurope/benchmarking/list/source_data_pdf/2nd_measurement_final_report.pdf
[3] See www.bcss.fgov.be
[4] See www.fedict.be

1. E-government: a structural reform process

The World Bank[5] defines E-government as the use of information and communication technologies (such as wide area networks, the Internet and mobile computing) by government agencies with the capacity to transform relations with citizens, businesses and other branches of government. These technologies can serve a variety of different ends: better delivery of government services to citizens (especially those living in remote or less densely-populated areas), improved dealings with business and industry, citizen empowerment through access to information and more efficient government management. The resulting benefits may be greater convenience, increased transparency and accountability in public decisions, revenue growth, less fraud and/or cost reductions.

Analogously with e-commerce, which allows businesses to trade with each other more efficiently (B2B) and which brings customers closer to businesses (B2C), e-government aims to make the interaction between government and citizens (G2C), government and business companies (G2B), government and employees (G2E), government and policy makers (G2P) and intergovernmental relationships (G2G) more friendly, convenient, transparent, and less expensive.

It is clear that the use of information and communication technologies is only a means to an end. The aim is to deliver better service to all stakeholders in government services. E-government is a structural reform process based on a view of information as a strategic resource in all areas of government activity. It implies a fundamental, customer-oriented re-engineering of the service delivery processes of government bodies as well as organizational changes within those bodies, an interoperability and security framework, co-operation between government levels and government bodies, adaptation of the law, education of customers, measures to prevent a digital divide, … In the following chapters, we give an overview of a number of preconditions for effective implementation of E-government.

This paper doesn't however pretend to be a global manual for the development of E-government initiatives. Important questions such as setting priorities, or programme and project management are not dealt with. A very interesting initiative in this respect, containing many links to best practice all around the world, is the E-government handbook published by the Centre for Democracy and Technology[6].

[5] See http://www1.worldbank.org/publicsector/egov/
[6] See http://www.cdt.org/egov/handbook/2002-11-14egovhandbook.pdf

2. Dealing with information as a strategic resource for all government activities

Information is a prime production factor for most government bodies. Government revenues such as taxes and social security contributions depend on data about the income of citizens and company revenues; elections can only be held based on information about people residing within a country's borders; benefits and subsidies are granted taking information about the living circumstances of the duly authorized person and his/her direct environment into account, …

Thus, it is very important that all government bodies deal with information as a strategic resource. This implies effective and efficient treatment of information in compliance with basic data protection regulations, such as the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[7]. Pure principles should be complied with on five topics.

2.1. Information modelling

Information should be modelled through government levels and government bodies in such a way that the model reflects the real world as closely as possible. This means the definitions of items of information, their attributes and interrelations is based on an abstraction from reality and not on legal concepts. In so doing, changes to the information model are avoided due to changing legal environments.

The information model should take into account as far as possible the likely uses to which information will be put. This requires a sufficient insight into the working of various government bodies, which can be ensured by creating a modelling committee that will agree on the information model and its subsequent changes.

Special attention should be paid to the time aspect during the information modelling process. The information may relate to a situation at a specific moment (e.g. the domicile on 1 January of a given year) or to a situation during a period (e.g. the salary relating to a certain working period). It is important to have consistency in the basic temporal units with which information is used for various purposes.

The real world changes continuously, and not all uses of information are foreseeable. Thus, it should be possible to extend or adapt the information model flexibly when the real world, or uses made of the information, change.

A good way to implement these information modelling principles is to use object-oriented information modelling techniques and modelling languages such as UML[8].

[7] Official Journal L 281 , 23 November 1995, p. 31. An electronic version can be found on http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm

[8] UML is the abbreviation of Unified Modelling Language. This language has been worked out by the Object Management Group (OMG). More information can be found on http://www.omg.org/uml/

2.2. Single collection and re-use of information

Information should only be collected by government bodies for well-defined purposes and in a way that is proportional to those purposes.

All information should be collected only once, as close to the authentic source as possible. Multiple government bodies should not be collecting the same information repeatedly from citizens or companies. Nor should they collect information from a source other than the one at which information was first created. For instance, an employer doesn't have to determine whether an accident which occurred at the workplace can be legally qualified as an industrial accident, but an industrial accident insurer must do so. Hence, this question must be addressed, not to the employer, but to the insurer.

Information should be collected using a channel chosen by the supplier of that information, but preferably electronically, using standard basic services (single sign-on, receipt upon arrival of a file, notification for each message, …).

Information should be collected in accordance with the information model and on the basis of uniform administrative instructions throughout all government bodies.

Ideally, the supplier of the information should have a facility to check the quality of information before passing it to a government body. This implies the public availability of governmental software to check its quality.

Once arrived at government, the information collected should be validated only once, following an established task sharing system, by the most suitably qualified government body or by the government body that has the greatest interest in its correct validation.

Only after this validation process, can information be shared and re-used by authorized users. Otherwise, errors will be distributed among government bodies. Moreover, suppliers of information risk being contacted by different government bodies to rectify the same incorrect information.

2.3. Information management

Information in all its forms (e.g. spoken, printed, electronic or image) should be managed efficiently throughout its life cycle.

Functional task sharing should be established, indicating which body stores which information in an authentic way, manages that information and makes it available to authorized users. In this way, an authentic source for every piece of information is set within the government as a whole.

Information should be stored in accordance with the information model and it should be possible to compile information flexibly in accordance with ever changing legal concepts.

Every government body has to report suspected information inaccuracies to the body that has been designated to validate that information.

Every body that has to validate information in accordance with the agreed task sharing system, has to examine any reported suspected inaccuracies, to correct them where necessary and to report the correct information to every government body known to have an interest.

Information should be retained and managed only while there exists a business need, a legislative or policy requirement, or - preferably in an anonymized or encoded format - when it has historic or archive importance.

2.4. Electronic information exchange

Once collected and validated, information should be stored, managed and exchanged electronically to avoid transcribing and re-entering it manually.

Electronic information exchange can be initiated by the body that holds information, the body requiring information or a service integrator (see point 6.2.).

Electronic information exchanges should take place on the basis of functional and technical interoperability framework that evolves continually but gradually in accordance with open market standards, and that is independent of the methods of information exchange used.

Available information should be used for the automatic granting of benefits, for pre-filling when collecting information and for information delivery to those concerned.

2.5. Protection of information

Security, integrity and confidentiality of government information should be safeguarded through an integrated set of structural, organizational, technical, physical, staff screening and other security measures in accordance with agreed policies.

Personal information should be used only for purposes that are compatible with the purposes for collecting the information.

Personal information should only be accessible to authorized bodies and users in accordance with business needs, legislative or policy requirements.

The authorization to access personal information should be granted by an independent committee, after having checked whether access conditions are met. Access authorizations should be published.

Each electronic exchange of personal information should be preventively checked for compliance with current access authorizations by an independent service integrator (see point 6.2.).

Each electronic exchange of personal information should be logged, to ensure the subsequent traceability of any abuse.

Each time information is used to take a decision, the information used should be notified to the person concerned together with the decision made.

Each person should have the right to access and correct personal data held about him/herself.

3. Customer-oriented re-engineering of service delivery processes of government bodies and value chain management

3.1. Customer-oriented re-engineering of service delivery processes of government bodies

E-government implies customer-oriented re-engineering of the service delivery processes of government bodies.

Firstly, this means that government bodies will have to shift, at least for those involved in service delivery to customers, from being an organization based on functional divisions towards a process-based organization. In so doing, the organization will become more flexible, more customer-oriented and the process approach will provide a basis for delegating responsibilities.

Customer-oriented process review of course means much more than merely deploying new technologies to sustain relations with citizens (G2C) and business companies (G2B). The provision of integrated electronic services through portals and other channels is important, but will only bring maximal added value if, at the same time, the processes within each government body and among government bodies (G2G) are redesigned from a customer-oriented perspective.

To shift towards a process-based organization, the processes need to be listed, described and organized to maximize added value to the customer. Such a process description should as a minimum give an answer to the following questions:

- ❑ which activities does the process consist of, represented in a sequence diagram ?
- ❑ does each activity of the process bring added value for the customer ?
- ❑ what production resources are involved in which activity ?
- ❑ what skills and knowledge are required to carry out each activity ?
- ❑ what is the processing time for each activity ?
- ❑ what are the relationships with other processes and activities, within or outside the own government body itself ?
- ❑ what improvements might be suggested for which activity ?

3.2. Value chain management

Customers are interested in services that are as fully integrated as possible when particular events occur. They want the processes offered by different bodies (government agencies, private companies,...) to be geared to each another in order to achieve maximum added value with minimum effort. In the case of relocation, for instance, they want all administrative formalities with the public sector to be settled through one single integrated process, and to be able to apply under the same process for services from private companies (i.e. electricity- and gas-distribution companies, removal firms, ...).

Moreover, customers wish the integrated services offered to them to join up perfectly with their own processes. For instance, they wish external obligations required when recruiting or hiring staff to be directly fulfilled by calling upon external processes using their own staff administration software.

Integrated services that join up perfectly with customers' own environments can be achieved by building chains of interlinked processes, so-called value chains. The government can co-ordinate the building of the value chains in some areas, but must also allow private companies and organizations to develop value chains, into which processes built by the government can be integrated. This presupposes that the government provides the processes built up in a well-documented way, and in such a way that they can be integrated within value chains developed by private companies and organizations.

Involving private companies and organizations in the delivery of public services can help the government increase take-up, improve efficiency and reduce the cost of government itself. The Belgian federal government will develop a framework for the integrated public-private supply of electronic services[9].

Under the value chain approach, integration of processes between government bodies, between government bodies and the private sector, and between government bodies and customers, is crucial. A lack of integration leads to overburdening customers by several government bodies repeatedly collecting the same information, unnecessary contacts with customers due to multiple, uncoordinated quality checks, efficiency and time losses within government bodies, sub-optimal support of the policy made by government and greater opportunities for fraud.

3.3. Principles to be taken into account to maximize added value for the customer

To maximize the added value of a service for the customer, the following principles need to be taken into account:

- ❑ a single declaration of each event during the life cycle/business episode of a customer implies automatic granting of all related services;
- ❑ declaration of events and service delivery takes place using an access method chosen by the customer, e.g.
  - interactive end-to-end integration with the customer's information system;
  - file transfer;
  - various end-user devices: PC, mobile phones, PDA, digital TV, kiosks, …;
  - use of intermediaries;
  - accessible to the disabled;
- ❑ when services cannot be granted automatically to a customer and are made available through end-user devices, they are granted
  - if possible, in a personalized way; this means, among other things,
    - o a look and feel that is adapted to suit the individual customer;
    - o presenting only relevant information and transactions to the individual customer;
    - o support that is adapted to the individual customer, e.g. by providing contextual help using language that is intelligible to the individual customer, on-line simulations, …

[9] A valuable policy framework in this respect has been elaborated by the Office of the e-Envoy at the United Kingdom. See http://www.e-envoy.gov.uk/oee/oee.nsf/sections/about-epolicy-intermediaries/$file/interm-index.htm

  - or at least based on the way of thinking of the group to which the customer belongs, e.g. based on
    - life events (birth, marriage, etc.) or business episodes (starting a company, recruiting staff, etc.);
    - life styles (sport, culture, etc.);
    - living status (unemployed, retired, etc.) or business sectors;
    - specific target groups;
- integrated customer relations management tools are used.

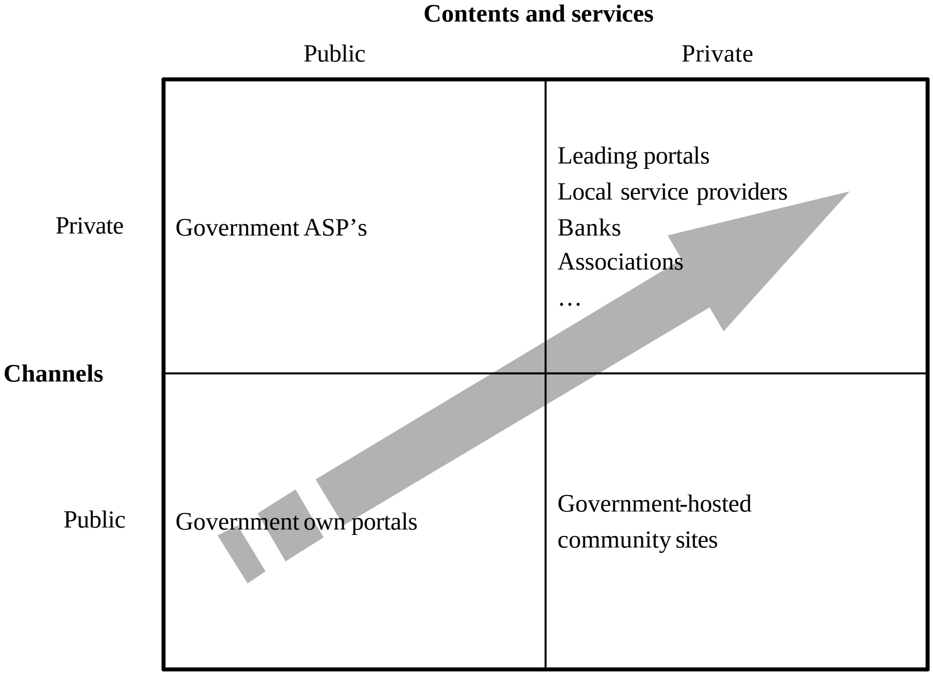
3.4. Implications for the development of web-based service delivery

3.4.1. Websites and portal sites

The above described view of customer-oriented service delivery based on value chains implies that the public sector is mistaken if he only offers his services from his own websites or portals. If each government level and body aspires only to that, customers will lack integrated services. Thus, information and transactions must be made available not only on their own website or portal, but need to be offered in such a way that they can be made accessible from each website or portal that citizens or companies wish to use. It might be websites or portals of other public levels, special-interest groups, financial bodies, sickness funds, ... It runs counter to an integrated customer-oriented approach to have public sector information and transactions offered only on public sector websites and portals, and to have information and transactions that do not come from the public sector offered only on non-public sector websites and portals. The diagram below, taken from a recent presentation by Gartner[10], clearly shows which trends might be expected as far as the ways of offering E-government services are concerned.

[10] See www.gartnergroup.com

Figure 1: evolution in the balance between roles in delivering E-government services



Source: Andrea Di Maio -Gartner

This implies the public sector needs to focus on the essentials when offering electronic services to citizens and companies.

When providing information, the public sector should

- issue it in generally available content management systems;
- make available modular, up-to-date information on the services it provides and the regulations it applies;
- with standardized metadata based on standardized thesauri;
- with separation of content and metadata (re-use, don’t rewrite);
- which can be submitted for automated re-indexing.

Regarding transactions, the public sector should provide components that integrate readily into websites and portals of the own government level, and those of other government levels or bodies and authorities outside the public sector.

Moreover, the Belgian federal government has chosen to offer an identification and authentication service to other government levels if they so wish, enabling citizens and companies to identify and authenticate themselves at all public websites and portals with the same user ID, password and token, providing they have followed a registration procedure. This identification and authentication service can be used until the electronic identity card (see point 5.2.) is available to all Belgian citizens. The registration procedure has been worked out by FEDICT for citizens[11] and the National Office for Social Security for companies[12]. The registration procedure for companies includes a facility to appoint trustees (i.e. social secretariats, accountants) who can act

[11] See www.belgium.be

[12] See www.socialsecurity.be

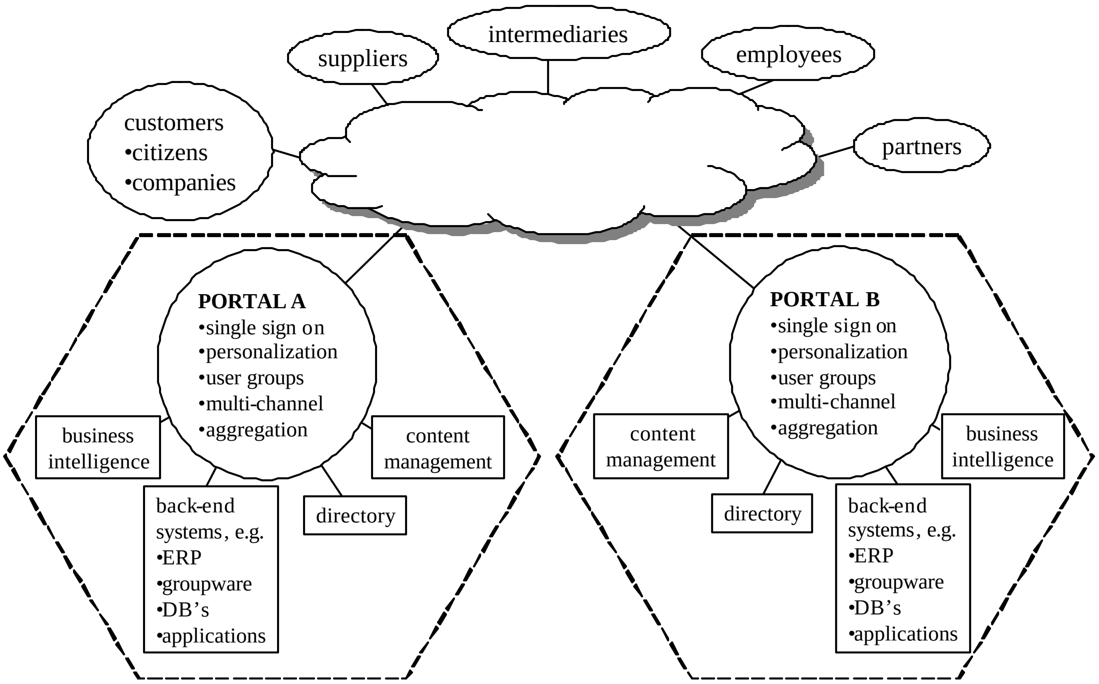
on the company's behalf. It is possible to call up the registration procedure from any public website or portal.

If government bodies develop their own websites or portal sites, they have to strive to achieve maximum added value for citizens and companies. This is possible by

- ❑ also making external information and transactions available through their websites and portal sites, so that users receive integrated services that match their needs as closely as possible;
- ❑ ensuring that information and transactions are accessible from as much relevant views as possible, chosen by the user;
- ❑ offering an integrated workflow to users, which can be integrated into their own workflow if they so wish;
- ❑ ensuring an integrated relations management with users through all the various channels (portal, e- mail, phone, ...), with feedback mechanisms in order to improve services continuously;
- ❑ striving for systems within which government bodies show citizens' and companies' entitlements and obligations in a pro-active and personalized way.

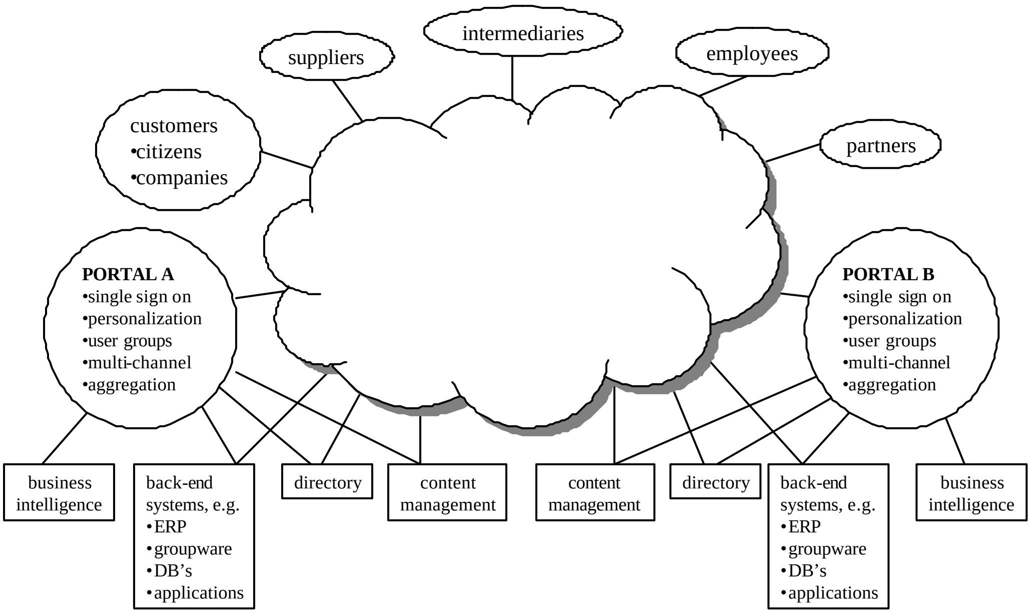
Below you will see two diagrams showing respectively which situation is to be avoided and which is to be achieved. In the first diagram, each portal site of a government body or government level only gives access to information and transactions of the government body in question or the government bodies belonging to the government level in question. Use of external directories is not possible. A customer has to register on various government portals and has to use particular identification and authentication methods on each portal.

Figure 2: portals: situation te be avoided



In the second diagram, each portal site of a government body or government level gives integrated access to own and external information and transactions. A customer has to register only once on a portal site he chooses and can use the same identification and authentication methods on all portal sites.

Figure 3: portals: situation te be achieved



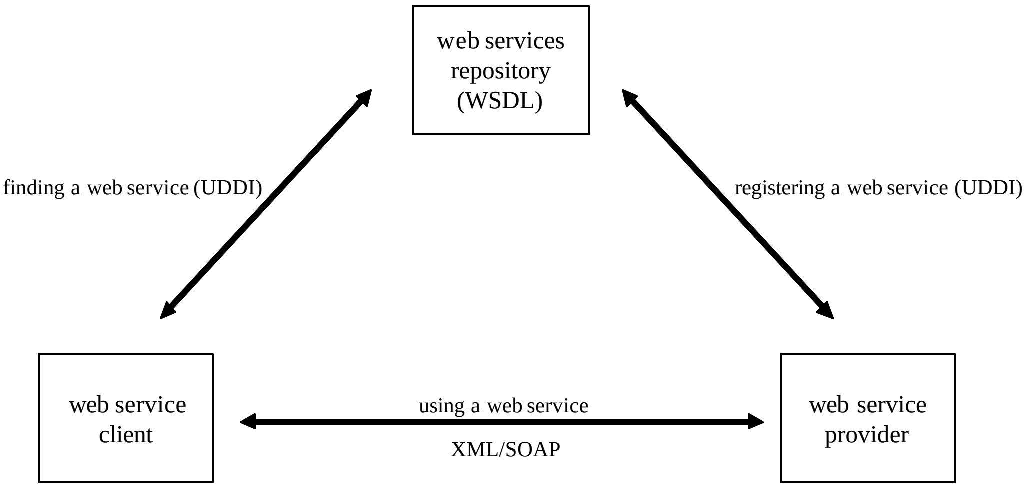
3.4.2. Application-to-application integration through structured messages and web services

Websites and portal sites are intended to be used by people. In an increasing number of situations, users of electronic services provided by the government will also want to integrate these services with their own computerized processes. The government must therefore also consider providing well-documented electronic services that can be called up directly from users' applications.

In its simplest form, structured messages can be published, through which applications of customers can communicate directly with government applications.

A next step is the publication of web services. A web service is a software component offering univocal, self-describing functionality, which can be called up in a distributed way using standard internet technology. The government then publishes the web services it offers in a repository. Interested users can consult the repository to find out the services available, functionality offered and how to use the services, and can have the web services called up through their applications. The diagram below shows how web services work.

Figure 4: web services


web services repository (WSDL)
finding a web service (UDDI)
registering a web service (UDDI)
web service client
using a web service
XML/SOAP
web service provider

3.5. Case studies

The Belgian federal administration has already earned some favourable reviews of processes and their integration into value chains. Three of these, the process re-engineering within the social security sector, the electronic application for a car licence plate and the Crossroads Bank for Enterprises, will be described below as case studies. In Belgium, these projects will serve as a model for future projects of the same kind.

3.5.1. Case 1: the social security sector

Belgian social security system consists firstly of three insurance systems (employees, self-employed workers and civil servants), covering a maximum of seven social risks (incapacity for work, industrial accident, occupational disease, unemployment, retirement, child care and holiday pay - the so-called social security branches), and secondly of four social support systems (allowances for the disabled, guaranteed family allowance, minimum income and income guarantee for the elderly), which grant people specific minimum services after verifying their subsistence resources. In all, about 2,000 social security offices are responsible for the delivery of Belgian social security. More than 10,000,000 socially insured persons and 200,000 employers have very frequent contacts with those offices to claim their entitlements, provide information and pay their contributions.

At the time, an in-depth analysis is of the functioning of social security proved that:

- the organization of social security offices' business processes was not very customer-oriented and was certainly not standardized among the various social security offices;

- each social security office had its own set of paper forms with accompanying instructions, on the basis of which, when a social risk occurred, one would request information that was specifically necessary to grant the entitlements in the light of that particular risk;
- social security offices very often asked the socially insured persons and their employers to request information that was already available at another social security office in the form of a paper document, and to produce that document, rather than exchanging the information directly among themselves;
- socially insured persons and their employers thus had to inform many social security offices of a single event, following different legal concepts and administrative instructions each time;
- socially insured persons and their employers themselves had to claim their entitlements throughout the social security system and could not count on the automatic granting of all entitlements on the basis of a single declaration.

Taking the above mentioned principles into account, a global review of the processes throughout the whole social security system has been carried out. The actual result can be summarized as follows:

- socially insured persons and their employers now need to make only a single declaration to the social security system as a whole in the following cases:
  - no later than the start of an employment relationship, an employer has to declare when (date and time) the employee in question takes up his duties;
  - every three months, the employer has to declare what income each of his staff has earned, divided into income components that from now are defined uniformly at all social security branches for employees and civil servants, and how many working days or equivalent days each of his staff has worked, divided into types of days that from now on are also defined uniformly at all social security branches for employees and civil servants;
  - when a social risk occurs, socially insured persons or their employers need only to declare information about that particular social risk; information on historic income, historic work performance or equivalent performance no longer has to reported as it is obtained from the quarterly declarations of wages and working time data; only if wages and working time data are necessary concerning a period for which the quarterly declaration has yet to be made, will the wages and working time data for this period still need to be reported in the form of an provisional declaration following exactly the same principles as the quarterly declaration;
  - no later than the end of an employment relationship, an employer has to declare when (date and time) the employee in question leaves the company;
- all declarations of the beginning and the end of an employment relationship have to be made electronically, either by exchanging XML messages between applications, or through transactions available at the social security portal, or over a voice server; declarations can be amended electronically, either by exchanging XML messages between applications, or through transactions available at the social security portal; each employer has access to his list of staff through transactions at the social security portal and can get an electronic list of his staff by file transfer in XML format, so that he no longer needs to keep up to date an own staff register;
- all quarterly declarations of wages and working time data have to be made electronically, either by exchanging XML messages between applications or

through transactions available at the social security portal; declarations can be amended electronically, either by exchanging XML messages between applications, or through transactions available at the social security portal;

- all declarations of social risks can be made either on paper or electronically, either by exchanging XML messages between applications or through transactions available at the social security portal;
- the elements included in the XML schemes have been defined uniformly in all declarations; the XML schemes per declaration can be downloaded from the social security portal; each three months, a new version of the XML schemes is made available, with a note of amendments compared with the previous version, taking any regulatory changes into account;
- all social security offices are connected onto a network for electronic information exchange managed by the Crossroads Bank for Social Security, and have a legal obligation to request all information available in the network from each other electronically;
- the Crossroads Bank for Social Security manages a reference directory, showing
  - for each citizen, at which social security offices he is known, in what capacity and for what period;
  - by type of social security office and the capacity in which a socially insured person might be known to that office, which types of data on socially insured persons are available;
  - by type of social security office and the capacity in which a socially insured person might be known to that office, which types of data that office needs and is authorized to receive from other offices in order to fulfil its duties;
- the Crossroads Bank for Social Security uses this reference directory
  - to ensure preventively that a social security office only gains access to data it is allowed to access, and on people who are known to it;
  - to route data requests to the social security office that can supply the data in question;
  - to transmit data reported automatically to the social security offices that can use the data in question to fulfil their duties.

The introduction of this system led to the following:

- about 170 types of paper documents which socially insured persons or their employers had to request at one social security office to pass it to another social security office have been abolished and replaced by direct electronic data exchanges between the social security offices in question; in 2002, 242.5 million concrete electronic data exchanges took place;
- about 50 types of social security declaration forms have been abolished;
- in the remaining 30 social security declaration forms the number of headings has been reduced on average to a third of the previous number;
- many declarations are made directly and electronically from employers' staff administration packs and accountancy packs;
- socially insured persons and their employers can make all social security declarations on the basis of a standardized apparatus of concepts and standardized instructions, and need to report data to the social security system as a whole only once;
- the number of contacts between the socially insured persons and their employers on the one hand and social security on the other has been drastically reduced;

- remaining contacts have been streamlined as a function of life events of the socially insured persons or events affecting the employment relationship between employer and employee/civil servant (entering service, performing work, falling sick, leaving the company, becoming unemployed, retirement, ...);
- personal services to employers and socially insured persons are provided;
- a great many subsidiary entitlements are granted using automated procedures, without the socially insured persons or their employers needing to make declarations anymore.

3.5.2. Case 2: car registration

Until recently, the only way to have a car registered in Belgium was to fill in a form, on which the following information and documents were asked for:

- data on the licence plate: number of a possibly already available licence plate, type of new plate being applied for;
- data on the vehicle: brand and type, cylinder capacity, power, frame number, European agreement number, fuel used for the vehicle, new or already used vehicle, date on which the vehicle was first used, colour of the vehicle, ...
- data on the applicant: name, first name, date of birth, address, phone (optional), fax (optional);
- proof that the vehicle vendor has fulfilled his fiscal obligations;
- an obliterated tax stamp;
- proof of the vehicle's compliance with technical requirements;
- the stamp of the insurance company insuring the vehicle and the name and signature of its representative;
- applicant's signature.

Before preparing a transaction to have such a request made electronically, one checked how the vehicle registration process might be rationalized in order to ask the applicant for as little information as possible.

Moreover, it has been proved that much of the requested information was already available in databases at the Ministry of the Interior, Ministry of Finance, Febiac (the Belgian federation of the motor industry) or private insurance companies. The information requested for an electronic registration of a vehicle could thus be confined to four number items, on the basis of which all other information required was available electronically from the relevant databases. These four numbers are:

- the applicant's single identification number;
- the vehicle frame number;
- the company number of the vehicle vendor;
- the company number of the insurance company insuring the vehicle.

In order to meet the wishes of the citizen or company, i.e. to drive a new car as soon and as easily as possible, a value chain was developed by setting up co-operation between the above mentioned public services and private organizations.

The transaction prepared for electronic registration of a vehicle is interactive. Each time one of the numbers is entered, on the basis of that number the application looks up the relevant database and displays the data found there. In this way, the user is alerted if he/she may have entered an incorrect number, and can take action to rectify any incorrect data held in databases.

3.5.3. Case 3: the Crossroads Bank for Enterprises

Setting up a company involves a great many administrative tasks which vary for example depending on the type of legal entity chosen, the type of business to be started up, whether staff are hired or not, ... Traditionally, the various administrative formalities had to be completed with various government bodies. Thanks to the creation of company counters and the Crossroads Bank for Enterprises, the foundations for integration of the relevant services to a budding founder of a company have been laid.

The amendments to this process have produced a position whereby, from now on, depending on the company's legal status, one and only one body is appointed to be responsible for a single collection of basic identification data concerning the company, its registration in the Crossroads Bank for Enterprises as well as any subsequent updates. This authority is called information manager. The information manager can indeed issue rules under which other bodies that know some items of information or amendments to them can record or amend basic identification data at the Crossroads Bank for Enterprises under its control.

The Crossroads Bank for Enterprises allocates each company and plant of that company a single identification number (see point 4.3.). Apart from the basic identification data and single identification number, the Crossroads Bank for Enterprises also includes references to authentic sources at other government bodies, or other items of information concerning companies and their plants.

The creation of the Crossroads Bank for Enterprises, appointment of information managers and creation of company counters has resulted in the following:

- ❑ each company will eventually deal with one and only one place to complete all the setting-up formalities;
- ❑ each company has a single number for all its governmental contacts, whereas in the past there were more than 70 types of identification numbers;
- ❑ each company has to notify its entire basic identification data to the government as a whole just once, and thus does not need to give the data repeatedly to different government bodies.

4. An interoperability framework

E-government implies the ability of government bodies, their staff, citizens and companies to share information and integrate business processes through the use of an interoperability framework. In this section, we describe the elements of such a framework.

4.1. Technical standards

Many international bodies and organisations elaborate permanently changing open ICT standards. Government bodies responsible for the co-ordination of E-government initiatives can benefit by using these standards as a basis for developing an interoperability framework. Such frameworks have been developed for instance under the United Kingdom Govtalk[13] initiative and the New Zealand E-government programme[14].

Typically, these frameworks set standards on

- ❑ interconnection: networks (TCP/IP), mail (SMTP), directory services (LDAP), data transfer (HTTP and FTP), …
- ❑ information exchange: structured data and open text (HTML and XML-schemes), locked text (PDF), data modelling (UML), data transformation (XSL), web services (SOAP, UDDI), service repositories (WSDL), …
- ❑ security: transport security (SSL), secure mail (S/MIME), digital certificates (X509), …

4.2. Agreements

Apart from technical interoperability based upon these standards, there is however a great need for agreement on how to ensure functional interoperability and how to ensure that investment made by parties won't become worthless each time standards change.

Topics to be treated within such agreements are

- ❑ standardized encoding (e.g. return codes, …);
- ❑ standardized use of objects and attributes;
- ❑ standardized layout of message headers, independently of the information exchange format (EDI, XML, …) or the type of information exchange (on line, batch, …);
- ❑ version management;
- ❑ backwards compatibility;
- ❑ SLAs on availability and service performance;
- ❑ access authorization management;
- ❑ anonymization rules;
- ❑ the availability of acceptance and production environments;
- ❑ priority management.

[13] See www.govtalk.gov.uk

[14] See www.e-government.govt.nz

4.3. Single identification keys

The exchanging of information could be greatly simplified and the accuracy of information exchange could be better safeguarded through the use of common identification keys within all (governmental) information systems. Of course, the presence of such keys makes it easier to interlink data. That's why we propose subordinating the interconnection of information to a previous authorization made by an independent committee. But when information exchange is allowed through such an authorization, it should take place in a way that best guarantees the accuracy of the information exchanged.

Each entity (e.g. a person, a company, a plot of land, …) that might be the subject of information management or exchange should have an identification key, with which the entity is identified within all (governmental) information systems. These identification keys should be

- ❑ single: this means each entity has only one identification key, and that the same identification key is not assigned to several different entities;
- ❑ exhaustive: this means every entity to be identified has an identification key;
- ❑ stable over time: this means the identification key doesn't contain variable characteristics of the identified entity, doesn't contain references to the identification key or characteristics of any other entities, and doesn't change when a feature of the entity being identified changes.

From an international perspective, either a country prefix can be added to the national identification keys, or conversion tables can be managed between national identification keys of different countries.

In Belgium, each private individual has a single identification number, allocated either by the National Register for private individuals registered in a Belgian population or aliens register, or by the Crossroads Bank for Social Security in the case of private individuals who have a file at a Belgian social security office or public service, but who are not or no longer registered in a Belgian population or aliens register. This single identification number is generally used as a common identification key by all government bodies. To ensure the uniqueness of the number, the National Register and Crossroads Bank for Social Security keep a set of basic identification data relating to people, to whom they allocate a number. Those data relate to the family name and first names, date and place of birth, address of the main residence, gender, nationality as well as date and place of death. The National Register also updates the marital status and occupation of the person concerned. Before allocating an identification number to a private individual, one first checks by consulting the available data whether the person concerned already has an identification number.

The identification number allocated to a private individual by the Crossroads Bank for Social Security is replaced by the identification number allocated by the National Register as soon as the person concerned registers him/herself in a Belgian population or aliens register. In this case, the link between the old and new numbers is held on a conversion table.

The basic identification data stored in the National Register or register of the

Crossroads Bank for Social Security are available for all government bodies that are thereby duly authorized by royal decree or, depending on the case, by the sector committee of the Commission for the Protection of Privacy created in the National Register or the Crossroads Bank for Social Security (see point 5.1.3.).

Since 1996, each private individual holding a single identification number has had a social identity card (the so-called SIS card). The SIS card is a memory chip card, on which the single identification number can be read visually or electronically. It has been designed by the Crossroads Bank for Social Security, and is distributed through the sickness funds. Apart from a single identification number, it also contains an indication - in electronic form - of the holder's insurability status in the health care sector. The insurability status must be known to some health care providers, such as pharmacists and hospitals, in order to fix the price the patient must pay for health care correctly. Before the introduction of the SIS card, the insurability status in the health care sector was proved with paper stamps, about 100 million of which the pharmacists and hospitals had to retype annually. Given that the SIS card's identification function will in the future be provided by the electronic identity card (see point 5.2.), we won't go into this card in greater detail. However, what is important is that each citizen in Belgium thus holds an official memory chip card, on which his single identification number can be read visually or electronically, and which he can use for identification purposes at each direct or indirect contact (e.g. through his employer) with the public sector.

In Belgium, since 1 January 2003 all companies and their plants have received a single identification number, allocated by the Crossroads Bank for Enterprises. For those firms that already had a VAT number before 1 January 2003, the company number is the VAT number. The notion of a 'company' is very broad, and includes every legal entity, as well as every private individual or organisation that practises a trade, deals on the market, is subject to social security as an employer or is liable for value added tax, also every self-employed person working as a service provider, working intellectually or practising a liberal profession. A private individual running a company thus receives, besides his single identification number as a private individual, a company number which identifies his company. The company number doesn't change if the company's owner or legal status changes. To ensure the number's uniqueness, the Crossroads Bank for Enterprises keeps a set of basic identification data relating to companies to which it allocates a number. It concerns the company name, addresses of its head office and its plants, its legal status and legal situation. Before allocating an identification number to a company, one first checks, by consulting the available data, that the company hasn't got an identification number yet. The basic identification data stored with the Crossroads Bank for Enterprises are partially available publicly. The non-publicly available data are accessible to all government bodies duly authorized for this purpose by the sector committee of the Commission for the Protection of Privacy created at the Crossroads Bank for Enterprises (see point 5.1.3.).

4.4. A shared, publicly accessible information model

As mentioned above, information has to be modelled, and to be collected, managed and exchanged in accordance with the model. The model typically contains standard elements, with well-defined characteristics, and the relations between those elements.

The model should be electronically and publicly accessible by a multiple-criteria search environment, with facilities to consult the model by element, scheme, version, …

The model should be the outcome of a participatory process between all parties dealing with the modelled information. Workflow should be available to validate standard elements and their characteristics.

To comply with current standards, the model should be object-oriented, i.e. permitting inheritance within a multilingual environment.

A very important aspect is version management within the model, allowing transparent and easy access to changes between versions.

Elements with their characteristics should be defined only once within the model, with a facility to view that definition in different formats.

5. A security framework and the electronic identity card

The extension of E-government presupposes that all users can justifiably trust in the security of the information systems used and the necessary measures to protect their privacy. This presupposes an integrated security policy throughout all government bodies, of which the protection of privacy is best treated as an integral part which fits in with the government's business continuity policy. The starting points and concrete design of such a policy according to ISO standard 17799 form a first section of this chapter.

Moreover, in Belgium, much attention is paid to elaborating a method that enables users of public services to identify and authenticate themselves electronically, and to place a qualified electronic signature within the meaning of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures[15]. This method is the electronic identity card, which is being distributed to private individuals registered in a Belgian population or aliens register. This will be described in the second part of this section.

This section is highly detailed. It reflects the vision of the Belgian federal government, under which the information security aspect and protection of privacy is a crucial factor for the successful implementation of E-government, and in accordance with which continual attention must be paid to it when reviewing processes and relationships.

5.1. Integrated information security policy

5.1.1. Starting points

Information security includes preventing damage that might be caused to the good functioning of government or services to its users, through the harmful effects on its methods and procedures on (electronic) information processing. The good functioning of government and the privacy of all those concerned are extremely important and valuable goods to protect. Appropriate measures are thus necessary to safeguard the integrity, availability, confidentiality (among other things the principles of purpose limitation and proportionality), non-repudiation, authenticity and auditability of information and information processing systems.

The computerization of government bodies and increasing collaboration relating to information management and process integration offers the prospect of great improvements in effectiveness and efficiency. But at the same time, new risks are being taken. Indeed, separate government bodies are no longer free-standing information processing entities, but rather parts of a coherent whole. With the growing collaborative connections, the risk of consequential damage and its extent on other systems is much greater than at the place where the original damage occurs. The vision of information security and protection of privacy must thus be determined collectively. Each ultimately responsible person at a government body is basically in charge of conveying this vision within his body.

[15] Official Journal L 13, 19 January 2000, p. 12.

Priority must be given to avoiding damage that might be caused to the proper functioning of government information systems on the one hand, and to the privacy of people concerned on the other. Prevention is the best method of protection. It is the action that prevents damage from occurring in the first place, by spotting and eliminating hazards in good time. Primary prevention precedes secondary and tertiary prevention, which, respectively, repair damage already caused and prevent any damage already caused from getting any worse. Nonetheless, the three forms of prevention are necessary because not all damage can be prevented, even with the best information security policy. When settling a security policy, it is necessary to keep this division in mind, because it shows how some simple and inexpensive measures may have more impact than expensive but less effective actions.

This leads logically to another security principle, i.e. risk assessment. Each advance and renewal results from separating good risks out from bad ones. The weighing of good and bad risks requires a reasoned approach: the chances of earning a profit must greatly exceed the risk of suffering losses. By raising security standards, it is possible to achieve a positive balance, but security also incurs costs that can seriously damage profits. The risk of losses must always be limited as far as possible, certainly, but at a reasonable cost. The efforts made concerning information security must thus aim at achieving the right balance between making a profit and avoiding losses arising from new actions. Absolute security cannot be presented as an ideal to pursue. Otherwise, every renewal risks being nipped in the bud.

The security of an information system is not a technical product which can be built into the system by experts, but results from careful execution of the daily tasks of each person who is affected by its proper functioning. He who wants to guarantee a secure future must in the first place take care of his own protection. That is why it is desirable to consider security as a value in the value framework of each government employee, as a goal to be permanently aimed at.

An expert can only give advice, point out tools, check, motivate, draw attention, be alert to the hazards to which the system to be protected is exposed. He must leave security itself to those who serve the system. It is they and no-one else who are the people ultimately responsible for protecting the system. The social organization of security is therefore a *condition sine qua non* of any security system. Not even the best technological tool can ever replace social control. It can undoubtedly improve security standards but, in the end, security depends on an efficient organization.

An information system is only as strong as its weakest link. A coherent set of measures is necessary, otherwise the effort made will be futile. That is why measures are necessary in the organizational, legal, technical and physical domains. Moreover, security problems have to be treated in a structured way and include essentially the following phases: an audit of the existing security situation, the setting of priorities in a security policy, practical application of the security policy into measures settled in a security plan, implementation of proposed measures, and permanent control aimed at verifying that existing measures are still needed and are being complied with.

It is impossible to propose any universal model solution for information security. A distinction must be made between general objectives which can be set globally, and the way to achieve those objectives. In choosing the way to achieve these objectives, one has to allow room to respond optimally to the real needs and risks of each environment. Rendering the people in question responsible by imposing controlled self-regulation on them within this framework is much more efficient than over-standardization imposed from above.

Security can hinder efficiency and user-friendliness, and is expensive. Moreover, the best preventive measures, i.e. measures relating to primary prevention, conceal all evidence of their own efficiency. Indeed, they don't allow damage to occur in the first place. Over the course of time, it gives a misleading impression of uselessness, resulting in lapses of attention and effort. This is precisely why permanent motivation, sensibilization and investment in information security are inevitable. One should constantly and consciously respond to the almost secular decline in preventive effort. This requires permanent boosts to security-mindedness, both for management personnel and their subordinates. It may well prove to be one of the most difficult tasks.

Ultimately, the information security policy must conform to current regulations concerning, among other things, protection of privacy and electronic signatures.

Put concretely, information security is best shaped on the basis of internationally accepted ISO standards; in this context, the most important ones are ISO standard 17799 (Code of practice for information security management) and ISO standard 15408 (Evaluation criteria for IT security).

5.1.2. Application in practice, in conformance with ISO standard 17799

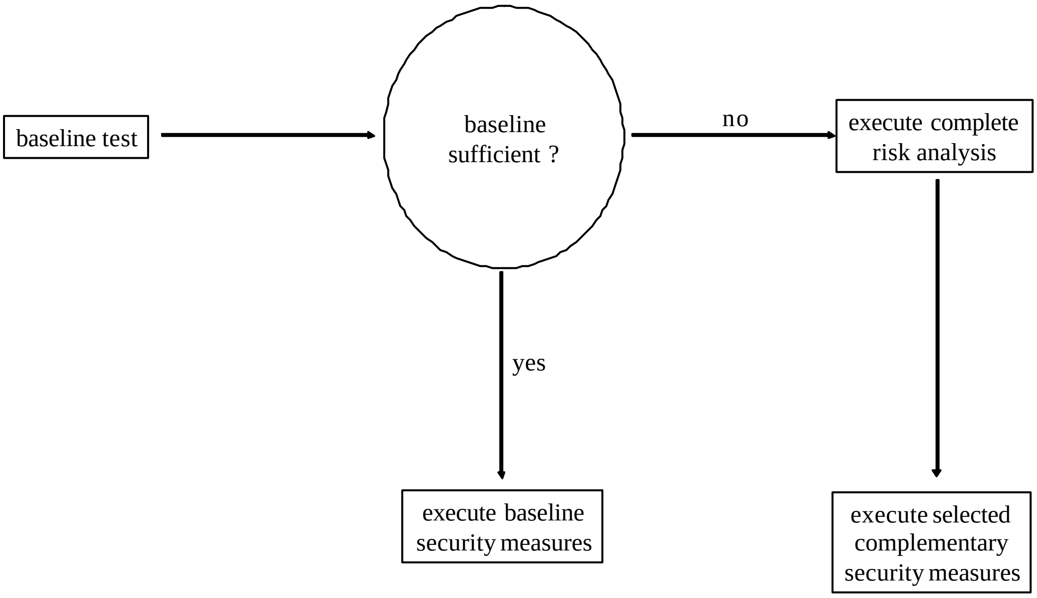
ISO standard 17799 includes ten main security domains. With regard to E-government, it should be supplemented by special measures on personal data processing and external communications on information security policy.
Measures relating to policy, organization, security requirements for staff and classification (the first four main areas of security under ISO standard 17799) are the building blocks for organizing information security. They thus take top priority. For the other areas, ISO standard 17799 gives three sources to set priorities:

- assessment of the greatest risks;
- external conformance analysis, i.e. conformance with what is prescribed by law or contracts, and what is good practice in the sector;
- internal conformance analysis, i.e. the consequences for information systems and their security resulting from changing business objectives (e.g. a government portal must be available 24/7, while delivering good performance).

To set priorities, it is advisable to carry out a baseline test. This implies verifying for each information system whether a set of baseline measures is considered sufficient as security measures, depending on the three sources mentioned. It is intended to carry out a detailed risk analysis only if those baseline measures appear inadequate.

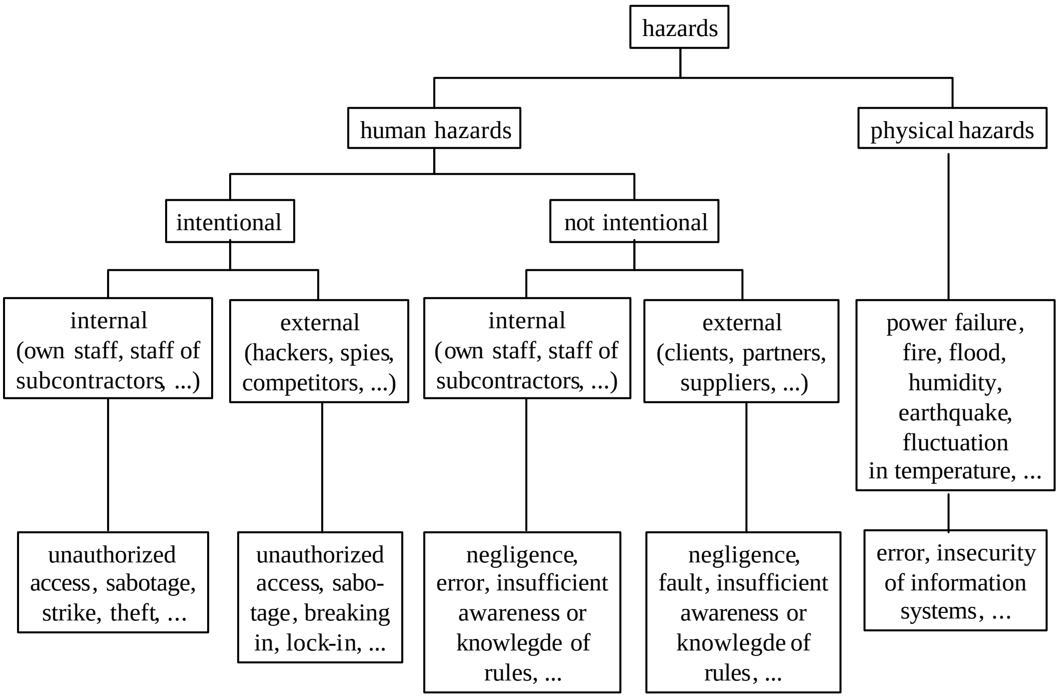
In the following diagram, this method is depicted schematically:

Figure 5: baseline test


baseline test
baseline sufficient ?
no
execute complete risk analysis
yes
execute baseline security measures
execute selected complementary security measures

When carrying out this risk analysis for information systems whose baseline measures are inadequate, the two risk aspects, i.e. the potential damage caused by an incident and the likelihood of such an incident occurring, must be compared against the cost of measures to eliminate the risk. The likelihood of an incident results from the potential hazards.

Figure 6: categories of hazards


hazards
human hazards
physical hazards
intentional
not intentional
internal (own staff, staff of subcontractors, ...)
external (hackers, spies, competitors, ...)
internal (own staff, staff of subcontractors, ...)
external (clients, partners, suppliers, ...)
power failure, fire, flood, humidity, earthquake, fluctuation in temperature, ...
unauthorized access, sabotage, strike, theft, ...
unauthorized access, sabotage, breaking in, lock-in, ...
negligence, error, insufficient awareness or knowlegde of rules, ...
negligence, fault, insufficient awareness or knowlegde of rules, ...
error, insecurity of information systems, ...

A detailed risk analysis might for instance be conducted in the following cases:

❑ for information and information systems that are especially vital to the government, e.g.
  - information systems used for information processing considered to be vital, critical, secret or confidential (see below, classification systems);
  - all front-office systems;

❑ situations where a security breach may have the following consequences
  - serious damage to confidence in E-government or the government itself;
  - risk to the security of their own staff, external people or groups;
  - serious deterioration in services provided to citizens and companies;

❑ situations where the losses from a potential incident exceed a pre-set figure.

5.1.3. Practical actions, by ISO standard 17799 domain, within the Belgian federal government

❑ organizational measures
  - a system of independent sector committees created within the Commission for the Protection of Privacy is being put in place; their duties involve authorizing the exchange of personal data by government bodies and social security offices, formulating recommendations and advice concerning information security and the protection of privacy, processing complaints from people concerned and arranging external audits;
  - all authorizations to exchange personal data are published on a (set of interlinked) website(s);
  - an information security and protection of privacy consultant is to be appointed at each government body (for smaller government bodies, it is possible to have a shared information security and protection of privacy consultant), with a

clear job description (including among other things the tasks of the data-protection official within the meaning of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and status; this consultant belongs to the Internal Audit Cell of the government body in question;
- a specialist information security service has been set up to support information security and protection of privacy consultants in fulfilling their duties;
- a Committee for Information Security has been set up, made up of information security and protection of privacy consultants from the various government bodies;
- a Steering Group for Information Security has been created, made up of a limited number of Committee for Information Security members and the departmental head of the specialist information security service; it acts as the driving force for the Committee for Information Security;
- each external electronic exchange of personal data by a government body or social security office is in principle (exceptions can be envisaged) preventively tested for compliance with their authorizations and logged by a service integrator, who is independent of the bodies affected by the data exchange;
- minimum security standards are being worked out by the Committee for Information Security and approved by the Council of Ministers, with an implementation date; each general manager of a government body must declare annually that his body complies with the minimum security standards; a false declaration is forgery, with sanctions as a possible consequence;
- the obligation to comply with security measures is automatically incorporated into contracts with third parties.

❑ security policies
- an integrated set of security policies is being elaborated through step-by-step refinement; directives, architecture, standards, procedures and techniques are being described to apply the integral set of security policies, in accordance with the priorities set by the Committee for Information Security; the policies always have the following structure:
  - material field of application: what the policy is all about;
  - personal field of application: to whom does the policy apply;
  - definitions of the concepts used under the policy;
  - general principles: setting rules and responsibilities;
  - requirements and references to other policies;
  - sanctions, arising among other things from regulations, if the policy is not complied with;
  - references to directives, architecture, procedures, standards and techniques to comply with the policy;
  - date of validation by the bodies concerned;
  - note of the person responsible for policy maintenance.

❑ classification of information
- the purpose of classifying information is to determine the protection level per information item, taking two aspects into account:
  - importance of the business continuity of public services (e.g. vital, critical, necessary, useful);

    - sensitivity in relation to protection of privacy (e.g. public, internal, confidential, secret);
  - the field of application of the classification exercise covers information (mainly personal data) used for services to citizens, companies and civil servants, regardless of the support equipment on which they are kept;
  - information is labelled depending on the classification criteria used.

- security requirements in relation to staff
  - security tasks and responsibilities are included in all job descriptions to which it applies; sensitive positions are stated as such in job descriptions;
  - applicants for sensitive jobs are screened carefully;
  - a secrecy declaration is signed by every staff member;
  - all staff members are briefed, educated and trained regarding information security and protection of privacy;
  - at each government body, robust procedures are settled and implemented to report any security breaches or weak points to the information security and protection of privacy consultant;
  - at each government body, a working method is settled and implemented to analyse any security-related incidents and weak points reported by the information security and protection of privacy consultant, and adequate remedial measures are proposed;
  - (disciplinary) sanctions are adequate when measures relating to the information security and protection of privacy are circumvented or not complied with;
  - it is checked that the (disciplinary) sanctions are sufficiently well-known when measures relating to the information security and protection of privacy are circumvented or not complied with;
  - it is checked that adequate measures are applied when a working relationship with a staff member is terminated.

- physical security of the environment
  - there are premises available that are well secured against malign external influences, unauthorized access, break-in, flood, fire, ..., and ICT infrastructure supporting vital and critical business processes is accommodated at these premises;
  - the electricity supply for ICT infrastructure supporting vital and critical business processes is guaranteed;
  - cables and air-waves are secured, especially against wire-tapping;
  - a procedure for the import and export of business equipment, among other things in cases of maintenance and repairs, is settled and implemented;
  - rules are settled for managing business equipment relating to people (e.g. laptops, handhelds, mobile phones, call tokens, ...) giving access to information that needs to be protected.

- communications and service processes management
  - the division of responsibilities for the management and maintenance of all parts of ICT infrastructure is settled and implemented;
  - security procedures, also procedures for resolving incidents, are settled and implemented, taking into account the necessary divisions of roles;

- the internal rules for day-to-day work (e.g. back-ups, banned use of computer games, code of practice regarding use of the Internet, closing of equipment, ...) are settled and complied with;
- each stage in the life-cycle of an application, including acceptance scenarios, is settled and complied with;
- new applications or amendments to existing applications are submitted for acceptance tests in an acceptance environment, separate from the production environment, before going into production;
- the six areas of ITIL methodology concerning service support, and first two areas of ITIL methodology concerning service delivery[16] are implemented:
  - service support
    - configuration management;
    - incident management;
    - problem management;
    - change management;
    - service/help-desk;
    - release management;
  - service delivery
    - service level management;
    - capacity management;
- there are preventive measures for the securing of all information systems against viruses and harmful software;
- procedures for information management supports (tapes, floppy disks, cassettes,...) are settled and complied with, including rules relating to:
  - storage and access;
  - shipping;
  - accidental destruction;
- networks are managed following well-defined procedures, especially when connected to external networks; in this respect, special attention is paid to
  - divisions between internal and external networks;
  - peripheral securing of internal networks (firewalls, ...);
  - authentication of components against one another;
  - intrusion detection;
  - application of encryption techniques where necessary;
- interchange agreements are written down for the use of network services, especially for network services used for external collaboration, including:
  - service level agreements concerning availability and performance;
  - demarcation of responsibilities relating to security and protection of privacy.

❑ processing of personal data

- for each processing of personal data, a controller, i.e. a person who determines the purposes and means of the processing and who is responsible for the processing, is appointed;
- personal data are processed in conformance with the principles of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data

[16] See http://www.itil-itsm-world.com

    and on the free movement of such data; the following principles are complied with:
    - purpose limitation principle: personal data must be collected for specified, explicit and legitimate purposes, and must not be further processed in any way that is incompatible with these purposes;
    - proportionality principle: the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed further;
    - data quality principle: data must be accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are processed further, are deleted or corrected;
    - reasonable storage duration: personal data cannot be stored longer than is needed to fulfil the purpose of the processing;
  - sensitive personal data, personal data relating to health, and legal personal data, are processed in conformance with the relevant special rules laid down by law issued in applying Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
  - the data processing controller informs the person concerned when personal data are collected, or when personal data are recorded/reported;
  - the data processing controller notifies the processing to the Commission for the Protection of Privacy, unless the processing is exempt from any such notification;
  - the data processing controller provides information to his staff members concerning data protection provisions;
  - the data processing controller regularly checks for conformance of information systems that process personal data with the notification made to the Commission for the Protection of Privacy;
  - procedures are settled and implemented to deal with persons exercising rights of access, reporting, correction, deletion, blocking access or objection.

- ❑ securing of access
  - an access management policy is settled and implemented, indicating among other things:
    - roles and functions;
    - authorizations on the basis of those roles and functions;
    - authorization time-limits;
  - authorizations are managed at the levels of:
    - people;
    - resources;
    - applications;
  - identification and authentication methods (user ID, password, token, digital certificate, electronic signature, ...) are set for people, resources, applications and services;
  - buildings are partitioned, securing rings are installed and access control measures to premises are implemented;
  - access control measures to physical resources (computers, networks, ...) by users (people, resources or applications) are set and implemented, with

particular attention to business equipment relating to people (e.g. laptops, handhelds, mobile phones, call tokens, ...);
    - access control measures to (sections of) application code are set and implemented;
    - access control measures to applications (parts) and services (parts) by internal and external users (people, resources or applications) are set and implemented (e.g. call-back procedures);
    - ICT equipment is automatically timed out after a set period of inactivity;
    - all access and actions carried out are time-logged.

- ❑ development and maintenance of information systems
    - security directives to be complied with during the development or maintenance of applications and services are set and implemented:
        - o division of functions;
        - o audit trails during development;
        - o documentation;
        - o regular interim back-ups;
    - the development environment is securized;
    - rules to build security into applications and services (e.g. validation of data input, checks of totals, verification of the authenticity of messages sent to subjects, ...), mainly externally accessible applications and services, are settled and applied;
    - procedures concerning technical and functional tests are settled and implemented in an acceptance environment, separate from the production environment, with clear go/no-go areas;
    - a method for analyzing the impact of amendments to operating systems on security and applications, on the permanent accessibility of information systems, and tests of the accessibility of information and applications in the amended environment before putting the amendments into effect, are settled and applied;
    - a method for analyzing the impact of amendments to standard software used on security and applications, and on the continuous accessibility of information systems, and tests of the accessibility of information and applications in the amended environment before putting the amendments into effect, are settled and applied;
    - a procedure for the destruction of information in the event that further processing is no longer authorized due to application of the proportionality principle or occupation of the country's territory, is settled and applied.

- ❑ continuity management
    - back-up procedures for information and applications are settled and applied;
    - the code and written documentation on the latest version of all applications is kept at a secure site outside the production location;
    - the parts of information systems, certainly those supporting vital and critical business processes, are split up at geographically dispersed sites (no single points of failure);
    - a business continuity plan exists at each government body and is made available to all those concerned
        - o indicating vital and critical components and processes;

        - with an inventory of necessary infrastructure and skills for each component and process;
        - with a description of actions, responsibilities and procedures in the event of an (internal or external) emergency;
        - with a description of continuation actions and procedures in the event of an emergency in order to return to normal operation;
        - with a description of test scenarios for the continuity plan with third parties affected;
    - the continuity plan is tested annually with the third parties affected and a report of the results is drawn up, aimed at permanent improvement;
    - the information systems for which this is justified are insured against physical risks such as fire, flood or earthquake, also against theft.

- ❑ internal and external checks
    - permanent internal check in respect of legislation, policies, directives, architecture, procedures and standards and on any undesirable use of ICT facilities (e.g. use of ICT for non-business purposes, ...) is carried out by the information security and protection of privacy consultant;
    - regular external check in respect of legislation, policies, directives, architecture, procedures and standards is carried out by an external auditor by order of the general manager of the government body or the Commission for the Protection of Privacy or the competent sector committee;
    - checking methods, and information systems and logs to be checked are, with the support of the ICT department, easily accessible to the persons carrying out internal and external checking functions;
    - monitoring systems, that raise potential risks linked to the infringements of the law, policies, directives, architecture, procedures and standards, and on any undesirable use made of ICT facilities, are available for the information security and protection of privacy consultant;
    - a regular check is carried out by the controller of the processing in respect of the security measures incorporated into contracts with third parties.

- ❑ notifying the public of the policy relating to security and the protection of privacy:
    - the integrated information security policy based on prevention, the information security structure implemented for this purpose, and the fact that for each E-government building block and project special attention is paid to security and protection of privacy, is reported to Parliament, and to the public through the press and publication on service integrators' websites;
    - when an E-government building block or project is presented to the public or to the press, special attention is paid to advice on security and protection of privacy, by producing the results of the risk analysis, measures taken to eliminate risks or to limit their impact, and the counterbalancing benefits that justify taking the residual risk;
    - together with the Federal Information Service, a communication strategy is worked out so as to be able, in the event of breach of security or protection of privacy, to provide information on the facts and to show what measures are being taken to prevent any further damage and prevent any similar damage in the future.

5.2. The electronic identity card

5.2.1. Explanation of a set of concepts

A *PKI* (abbreviation of Public Key Infrastructure) is a system that makes *digital key pairs* (always consisting of a private key and a public key) available to users of electronic communication services, with which they can protect and authenticate their electronic communications (i.e. to guarantee that the communication comes from a specific source and has not been amended after being sent from that source).

Securing and authentication through the use of digital key pairs is based on the principle of *asymmetric encryption*: that which has been encrypted with the private key can only be decrypted with the corresponding public key, and the converse. The private key of a key pair may only be used by the holder of that key pair, and hence must be kept safely. The public key of the key pair may possibly be used by each potential contact person of the private keyholder, and will thus be publicly accessible in a database.

If key pairs are used to authenticate electronic communication (i.e. to guarantee that the communication comes from a particular source and has not been amended after being sent from that source), they are unambiguously linked to one or several *certificates*, on which the identity and/or one or several characteristics of these source are shown.

Digital key pairs made available by a PKI infrastructure can be used for various purposes, such as encryption of messages (to safeguard confidentiality and integrity), authentication when consulting websites, placing qualified electronic signatures with legal force, … In general, however, it is argued for security reasons that a key pair used to place an electronic signature with legal force should not also be used for authentication when accessing websites, nor for encryption purposes.

In distributing certificates, two roles can be distinguished:

- ❑ the role of the *registration authority (RA)*: the RA is the counter at which the certificate is requested; it verifies that the identity or characteristic given is correct; if this is the case, it approves the request and informs the certification authority to that effect;
- ❑ the *certification authority (CA)*: on the basis of information received from the RA, the CA issues a certificate which it links to a key pair, showing exactly what that key pair will prove from that time on.

In addition, there is also the role of the *directory service (DS)*, which publishes certificates (containing the corresponding public keys) which have been issued by a certification authority and, possibly, also the contents of those certificates. The current status of a certificate can be verified by using an *OCSP (Online Certificate Status Protocol) responder* which immediately answers whether the certificate in question is still live or not (i.e. is suspended or even permanently cancelled).

An *electronic signature* is a legally valid electronic alternative to a handwritten signature. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (see point 7.3.)

imposes on Member States of the European Union a duty to adapt their law to give legal force to electronic signatures under certain conditions. At the present time, the most widely used technique for the creation of an electronic signature is the technique of digital key pairs with associated certificates.

A certificate can prove the keyholder's identity and/or one or several characteristics of that keyholder, such as qualifications (e.g. a qualified doctor), positions (e.g. president of the Federal Public Service Justice) or mandates (e.g. the right to execute financial operations up to a certain amount). Traditionally, a handwritten signature only proves a person's identity, not any of that person's characteristics. Characteristics are not proven with a hand-written signature but by other means (e.g. the function shown below the signature). To allow a person to use the same key pair and associated certificate to place an electronic signature with legal force regardless of qualification or position, the certificate should only contain information on the identity of the person concerned, and not on his/her characteristics. Including information on characteristics in a certificate linked to key pairs used to place an electronic signature is sub-optimal because it restricts general use of the signature.

5.2.2. The electronic identity card

The Belgian electronic identity card has the following functions:

- ❑ visual and electronic identification of the cardholder;
- ❑ electronic authentication of the cardholder using the digital key pair technique;
- ❑ generating an electronic signature with legal force by the digital key pair technique (non-repudiation);

The Belgian electronic identity card thus does not function as an electronic currency. Encryption key pairs are not yet envisaged either.

The Belgian electronic identity card takes the form of a processor chip card. On the one hand, data are printed on the card, and on the other, data are stored on the card's processor chip.

The following data are printed on the card, and can thus be read visually:

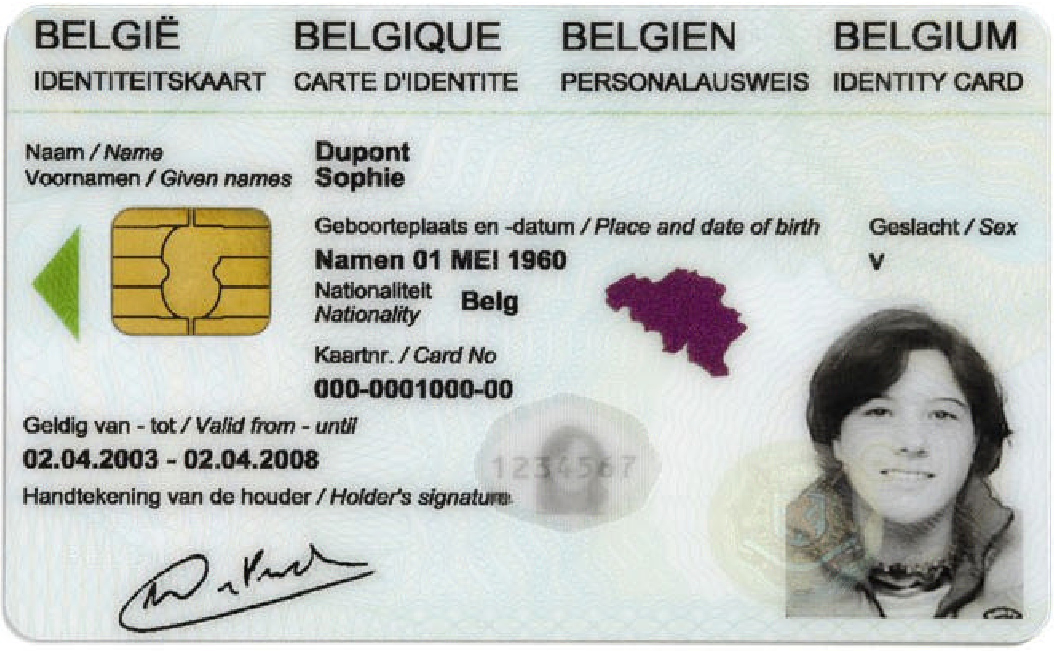
- ❑ the cardholder's single identification key, i.e. his national register number;
- ❑ the identity card number;
- ❑ the cardholder's basic identification data (name, first names, gender, date and place of birth, nationality);
- ❑ the cardholder's main residence (a transitional measure until 1 January 2004);
- ❑ a photograph of the cardholder;
- ❑ the handwritten signature of the cardholder and the municipality official;
- ❑ the card's period of validity;
- ❑ place of card issue.

The following data are entered on the processor chip of the card, and can be read electronically:

- ❑ the cardholder's single identification key, i.e. his national register number;
- ❑ the identity card number;
- ❑ the card's serial number;

- the cardholder’s basic identification data (family name, first names, gender, date and place of birth, nationality);
- the cardholder’s main residence;
- a photograph of the cardholder;
- the card’s period of validity;
- a private key with a corresponding certificate that can be used for electronic authentication of the cardholder;
- a private key with a corresponding certificate that can be used by the cardholder to place an electronic signature with legal force.

Figure 7: the electronic identity card



BELGIË BELGIQUE BELGIEN BELGIUM

IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD

Naam / *Name* **Dupont**
Voornamen / *Given names* **Sophie**

Geboorteplaats en -datum / *Place and date of birth* **Namen 01 MEI 1960**

Geslacht / *Sex* **V**

Nationaliteit *Nationality* **Belg**

Kaartnr. / *Card No* **000-0001000-00**

Geldig van - tot / *Valid from - until* **02.04.2003 - 02.04.2008**

Handtekening van de houder / *Holder's signature*

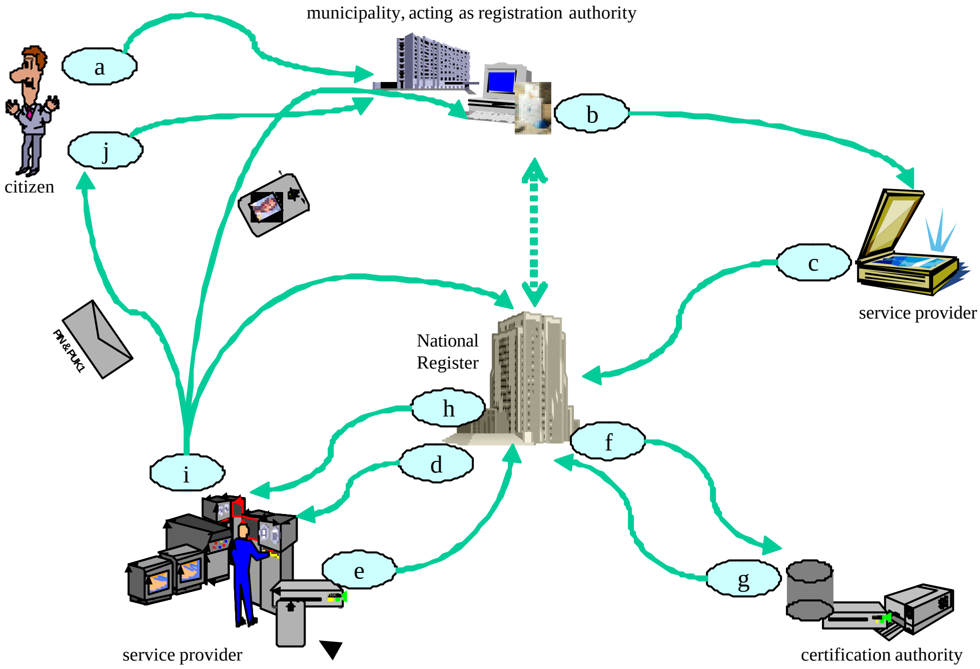
The use of private keys and the corresponding certificates is secured by a PIN code. To place a qualified electronic signature, the PIN code must be entered each time a signature is to be placed. For authentication and to place an electronic signature, no call is made to verify biometric properties (e.g. digital fingerprint, voice recognition, …). The use of biometry is not yet considered feasible on such a large scale, among other things because of the need for complicated and expensive ancillary equipment.

No other data than those mentioned above are stored on the processor chip of the electronic identity card. Indeed, a conscious decision has been made to use the electronic identity card only as a means of identification, authentication and to place a qualified electronic signature, and not as a means of transmitting data. It is a deliberate choice to transmit data over networks, with the card as identification and authorization methods to give access to data relating to the cardholder. Indeed, storage of data on the card itself would imply the cardholder needed to update those data whenever they change. Electronic data exchange over a network relieves the cardholder from regularly updating the card and offers the user of the data greater safeguards with regard to data availability and quality.

On the basis of a call for tenders, the government has on the one hand chosen a service provider to produce electronic identity cards, and on the other a certification authority to produce certificates. Municipalities serve as local registration point to issue certificates. In practice, this means municipalities act as service counters for electronic identity cardholders, and identity checks required to issue the identity card are also used to issue the certificates.

The following diagram illustrates the practical process to issue and deliver an electronic identity card:

Figure 8: process to issue and deliver an electronic identity card



a) when summoned by the municipality for this purpose, the citizen turns up at the town hall with a mug shot; the competent municipality official prints out an official document containing basic identification data and the main residence of the person concerned, certifies the accuracy of the data by comparing them against the data held on the municipality population register, sticks the mug shot onto the document and signs the document; the citizen indicates on the document whether or not he/she wishes to use the electronic identity card for electronic authentication and to place qualified electronic signatures, and signs the document in turn;

b) the document is sent to the service provider, who digitalizes it;

c) the duly digitalized document is sent to the National Register; the National Register prepares a file with data that are to be printed on the card visually, as well as a file with data that must be stored on the card electronically;

d) the National Register orders the issue of the electronic identity card and passes the prepared file to the service provider; the service provider then
   - issues a card;
   - initializes the processor chip with the file containing the data that are to be stored on the card electronically;

- generates three key pairs in the processor chip which will be used in future to authenticate the card, authenticate the cardholder and enable the cardholder to place a qualified electronic signature; the private key of the three key pairs cannot leave the card;
- personalizes the card by burning the data that are to be shown visually onto the card;

e) the service provider sends the public keys of the key pairs to the National Register, as well as the file stored in the card's processor chip and the data needed to identify the processor chip; the National Register checks that the public keys are unique, verifies that the file stored in the processor chip is correct and generates the serial numbers of the two certificates;

f) the National Register instructs the certification authority to issue the two certificates; the certification authority issues the certificates, stores them in a database and makes them publicly accessible if the citizen has indicated that he/she wishes to publish his certificates;

g) the certification authority passes the two certificates to the National Register; the National Register generates a set of digital signatures enabling completion of the initializing of the processor chip, also to determine the authenticity of the data entered onto it subsequently;

h) the National Register passes the digital signatures thus generated to the service provider, as well as the two certificates, if the citizen has indicated that he/she wishes to use the electronic identity card for electronic authentication and to place qualified electronic signatures; if this is not the case, the National Register keeps the two certificates in a database; the service provider stores the data received in the card's processor chip, generates a PIN code and two unblocking keys (PUK1 and PUK2) at random, and blocks the electronic identity card;

i) the electronic identity card is sent by the service provider to the official responsible at the municipality where the citizen lives; the PUK1 and – if the citizen has indicated that he/she wishes to use the electronic identity card for electronic authentication and to place qualified electronic signature– the PIN code are sent by the service provider to the citizen; its dispatch is reported to the National Register;

j) the citizen turns up at the town hall with his/her PUK1 code and, if necessary, his/her PIN code; the municipality official enters the PUK2 code he/she has received from the National Register together with the citizen, who enters the PUK1 code to activate the card; the citizen can read the contents of the processor chip to the end; if the citizen has indicated that he/she wishes to use the electronic identity card for electronic authentication and to place qualified electronic signatures, he/she can test those functions.

In order to have the electronic identity card considered a secure method of placing a qualified digital signature within the meaning of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, it will be tested by a body competent for that purpose, in conformance with the requirements laid down in annex III to this Directive.

In addition, the certification authority chosen by the administration requests its accreditation by a body competent for this purpose, to verify whether the authority itself and the certificates it issues comply with annexes I and II of Directive

1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Finally, in order to give guarantees to users of the electronic identity card regarding the proper functioning of the reading devices and corresponding electronic identity card software, a registration procedure for the devices and corresponding software has been promulgated by royal decree. This procedure will be combined with the already-existing registration procedure for the reading devices and the corresponding SIS card software[17].

The electronic identity card can be used as a minimum for the authentication of citizens and to place an electronic signature in relation with the public sector. Citizens and private companies can also agree to use the electronic identity card for the same purposes as part of their own relationships. Belgian banks, for instance, are very interested in this application. At present, each bank is obliged to keep a database with the identification and authentication methods of each of its clients; they won't risk having one client running off with another client's money. To make identification and authentication watertight, each bank must make a huge investment. The electronic identity card resolves this problem for them. As the electronic identity card is designed to be read by any CZAM terminal (the card reader standard followed by the Belgian banks) any bank clerk can verify the identity and authenticity of any Belgian client at any time. And at the same time, each document can be signed electronically. The card readers themselves form a common business case: the administration is interested in having as many as possible certified card readers on the market at the most attractive price, so that the threshold for use of electronic identification and authentication will fall as low as possible. The private sector will supply the card readers.

[17] This procedure is documented on www.ksz.fgov.be, rubric SIS-kaart, headword Leesapparatuur van de SIS-kaart.

6. Implementation with a decentralized approach, but with co-ordinated planning and programme management and permanent co-operation between government levels and government bodies (think globally, act locally)

In most countries, numerous bodies play a part in the provision of services of general interest. This concerns government bodies as well as private companies. Moreover, most countries do not have just a single tier of government. In Belgium there are no less than five tiers: federal level, community level, regional level, provincial level and the municipality level. Each of these tiers is responsible for particular domains of public services.

Each government body and private company having a duty of general interest necessarily develops its own dynamics regarding electronic service delivery, which enables the implementation of initiatives using a decentralized approach.

However, citizens and companies wish to receive integrated services across all bodies affected. Integration of processes must make it possible to develop the necessary transparency for clients with regard to governmental organization. Finally, customers are not interested in organization as such, but by the services delivered. This is why it is important that a shared vision exists among government levels and bodies, and that the necessary co-ordination exists concerning programme and project management. In Belgium, a co-operation agreement has therefore been concluded between the various government levels.

6.1. The co-operation agreement between government levels

6.1.1. Introduction

Successive State reforms have not simplified the integration of processes in Belgium, but have rather made the need even greater. Many services demand action by different authorities: the municipality, province, community, region, federal level and Europe. It has become almost impossible for citizens or companies to know to which authority they must address which question. In many cases, only an integrated approach can offer a complete answer to the questions posed by citizens and companies.

That's why, within the E-government policy of the Belgian federal government, one soon started to seek specific co-operation with different communities and regions. In March 2001, these efforts eventually resulted in the co-operation agreement between the federal State and the communities and regions with regard to constructing and operating a common E-platform[18].

This co-operation agreement was signed by the Federal State, Flemish Community, French Community, German-speaking Community, Flemish Region, Walloon Region, Region of Brussels-Capital, Flemish Community Commission, French Community Commission and Common Community Commission.

[18] See http://www.belgium.be/eportal/application?pageid=contentPage&docId=20434

When this co-operation agreement was signed, the wish to involve the provinces and municipalities in the extension and operation of the E-platform was also expressed.

6.1.2. Objectives

The aim of the co-operation agreement's signatories is to use information and communications technology to transmit information to all citizens, all companies and other organizations and authorities in a user-friendly way, and to give them an opportunity to carry out electronic transactions with the authorities in a trusted, secured environment. Therefore, all the parties' data and services had to become jointly accessible, and offered through various communication channels to the citizens, companies and other organizations, and to the parties to the co-operation agreement.

6.1.3. Contents

Under this co-operation agreement, the parties undertake to co-operate in the field of the building, co-ordinating and operating an integrated E-platform. The E-platform has been defined as an electronic platform facilitating rapid, direct communications between government and citizens, companies and other organizations, as well as among the parties themselves.

In order to achieve those shared objectives, the signing parties undertake:

- to offer electronic services based on intentions (intention-based services – customer-centred services);
- to work using the same navigation structure and taxonomy for all intention-based services involving the various parties or existing at the various government levels;
- to develop the necessary infrastructure (portal and middleware) themselves, or to appeal to possible common initiatives to this end, in such a way that it can transparently form part of the integrated E-platform;
- to take into account all the necessary agreements, standards and norms, among other things concerning the use of open and scalable solutions;
- to develop an integrated PKI (Public Key Infrastructure) initiative for E-government, and to use the single identification keys for citizens and companies.

Therefore, the signatories undertake to develop an integrated platform to build and manage portal sites with the following functionalities:

- a search engine, i.e. an application allowing a search for information at the portal and websites to which references are given from the portal;
- a content management tool, i.e. an application making it possible dynamically to manage the portal's contents and the links to websites to which references are given from the portal;
- an interface with different types of access channels, such as the web, telephone, mobile phone, digital television, or others from which the user can choose.

With this integrated platform, it is possible to develop intention-based portals at which references to information and transactions at all government levels are given.

In addition, it has been agreed to develop an integrated middleware environment that can be used to organize the exchange of structured electronic messages between three types of components

- portals;
- websites;
- back-end information systems.

These three types of components of all the signatories' government bodies can receive and send electronic messages from and to the integrated middleware environment, either directly or indirectly through their own middleware environment.

The parties concerned can decide freely whether or not to use, for the exchange of structured electronic messages between components at their own level, a common middleware environment against payment of the relevant charges, or to use a middleware environment under their own management for this purpose.

The integrated middleware environment is based on the IP telecommunications protocol and the XML protocol for data structures. For each structured electronic message, content structure is determined in consultation between the parties concerned.

As already mentioned, the aim of the signatories to this co-operation agreement is also to gradually use single identification keys in relations between bodies of the same government level, between bodies of different government levels and between government bodies on the one hand and the citizens and companies on the other. These single identification keys are:

- the National Register number for private individuals who have such a number, provided that the government bodies are authorized to use it in conformance with the applicable legislation;
- the company number allocated by the Crossroads Bank for Enterprises for companies;
- a number jointly agreed for any other entities.

All signatories to the co-operation agreement also will accept the methods worked out by the federal government and approved in the National mixed commission for the removal of obstacles to the information society, to authenticate customers and to obtain electronic signatures.

In addition, it has been agreed under the terms of this co-operation agreement that internal business processes should be settled by the government level in question. The business processes of various government levels must be co-ordinated for the processes for which it is useful for reasons of global efficiency, cost control or integrated services to citizens or companies.

It has also been agreed that task assignments will be determined gradually, regarding the management of data in an authentic form, taking into account the current distribution of competences between government levels. This means that for each data category, it is agreed which public service will store and update those data as being the authentic source, taking into account as far as possible the needs of all other government bodies. Other government bodies needing those data then know where to find them. They just have to store them for the period necessary to fulfil their duties, and they don't have to worry about updating the history.

If a government body other than the authentic source knows of an error or an amendment to an item of data, it must immediately report it to the authentic source, who will then take action as required. Where possible, government bodies acting as the authentic source for data will automatically transmit amendments or corrections to those data to the other government bodies that need them to fulfil their duties.

As this assignment of tasks is carried out, it will be translated into a data model to be settled jointly. This data model only concerns data that are common to the signing parties.

It has also been decided that, in consultation with the parties to this co-operation agreement, common policies will be settled in the following areas:

- authenticity;
- confidentiality;
- privacy;
- security;
- service level agreements.

Moreover, the parties also undertake to agree to what extent they wish to adopt directives for a common 'look & feel' and the user interface of websites and contact centres that come within their competence.

Finally, it has been agreed that, regarding access (user media) and distribution, the common E-platform will adopt a technology-neutral position, so that co-operation with all current and future types of service providers and the use of all kinds of end user devices, such as phone, TV, PC, kiosks or others, will be possible. This technology neutrality applies firstly to communications between the common E-platform and the parties.

6.1.4. Management and working practices

In order to apply this co-operation agreement, it has been decided to create a technical working group, made up of one representative of each party concerned.

The chair of this technical working group will be rotated each six months by one of the parties.

At present, this technical working group works in two domains: content management and the technological architecture of the integrated E-platform.

Within the 'content management' domain, a common portal navigation structure and a common taxonomy is being developed. Practical value chains, such as those for starting companies up and the awarding of subsidies, are also being worked out.

Within the area 'technological architecture of the integrated E-platform', the architectural components described above are being settled.

6.1.5. Cities and municipalities

The signatories to the co-operation agreement have very clearly expressed their wish to involve cities and municipalities in the integrated E-platform as well. Indeed, cities and municipalities are – certainly for citizens – the most frequently contacted government level in Belgium.

This is also why, under the terms of the co-operation agreement, the federal government seeks to conclude practical agreements with cities and municipalities regarding the content management level (processes) as well as the technological architecture level.

Some examples of this are:

- working out a common provisional authentication mechanism until the electronic identity card is available to all Belgian citizens, enabling citizens to register themselves only once, and to be authenticated so as to be able to correspond with any government level;
- working out practical applications for the electronic identity card, such as access to the public library in a particular city or municipality, access to skip parks, and so on;
- working out transparent processes, such as an application for a building licence, where all government levels in Belgium may be involved.

6.2. Towards a network of service integrators

In concrete terms, the co-operation between government levels in Belgium will lead to an ever expanding network of service integrators. A service integrator is a body that is both the motor and co-ordinator of E-government initiatives at a specific government level or a specific sector of the public services (e.g. social security). Typical duties of a service integrator are

- to stimulate and settle programmes and projects at the government level or the sector of public services in question, in accordance with the shared vision;
- to manage programmes and projects at the government level or the sector of public services in question;
- to develop and manage basic services in order to sustain integrated services to citizens, companies and their representatives, such as
  - a physical network to which all the bodies of the government level or sector of public services in question are connected;
  - a secure messaging system implemented over that physical network;
  - business logic and workflow support;
  - a portal environment including a content management system;
- management of a directory of authorized users and applications, containing:
  - a list of users and applications;
  - a definition of authentication methods and rules;
  - a definition of authorization profiles, indicating which service is accessible to which type of user/application regarding which persons/companies in which capacities, in what situation and for what periods;
- management of a directory of data subjects, indicating which persons/companies in which capacities have personal files with which bodies and for what periods;

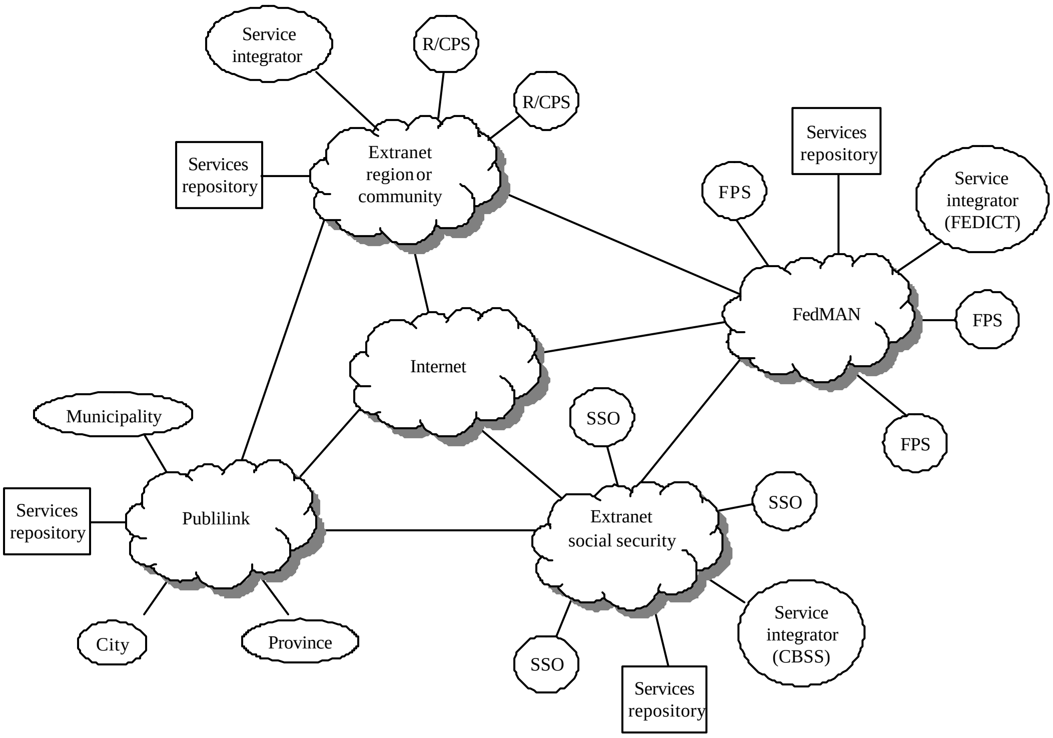
- management of a subscription table, indicating which users/applications want to receive which services automatically, in which situations, for which persons in which capacities;
- to preventively check each electronic exchange of personal information by a body of the government level or sector of public services in question for compliance with current authorizations granted by the competent independent committee;
- publication of the services provided by the government level or the sector of public services in question in a service repository which is publicly accessible, so that those services can be used by interested customers within and outside the government level or sector of public services in question.

Service integrators will co-operate closely, including in the following areas:

- they will conclude agreements on the vision between themselves;
- they will jointly co-ordinate their programmes and projects;
- they will connect their basic services to one another;
- they will jointly agree on work distribution concerning specific areas such as the development and management of basic services, so that on the one hand economies of scale are achieved, and on the other so that citizens, companies and their representatives get an assurance that they will not have to go through the same routine several times for basic services with different service integrators (e.g. by using shared directory services, one avoids having the same citizen or company needing to register himself/itself in several directories).

The Belgian network of service integrators can be visualized diagrammatically as follows:

Figure 9: network of service integrators



In practice, in Belgium FEDICT plays the role of service integrator between the federal public services, and the Crossroads Bank for Social Security plays the role of service integrator in the social security sector.

7. Revision of the legal framework

7.1. Legal embedding of the principles regarding strategic use of information

To make the use of information as a strategic resource (see point 2.) enforceable by citizens, companies and among government bodies, these principles should be formalized in law.

Some principles, such as the fact that information can only be collected by government bodies for well-defined purposes and in a way that is proportional with those purposes, also most of the principles concerning the protection of information, are mentioned in the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The regulation on data protection of all Member States of the European Union thus normally includes these principles.

New regulations are needed to enforce the other principles. Typically, the principles will come into effect gradually, as the necessary implementation measures are undertaken. To indicate a clear intention to comply with the principles, the regulation should prescribe that the principles have as a minimum to be complied with on every new government initiative.

Models of such regulations can be found in the Law of 15 January1990 concerning the creation and organization of a Crossroads Bank for Social Security,[19]also in clause 102 of the Programme Law of 30 December 2001[20].

Typically, such a regulation provides a legal basis

- to determine functional task sharing for the validation, storage and management of information between government bodies;
- to require government bodies to implement the electronic collection of information from other government bodies if the information is already available at the last mentioned bodies;
- to require government bodies to implement the electronic transmission of information they hold to other government bodies that need this information in order to fulfil their duties;
- to permit or require the use of single identification numbers;
- to define modalities for collection and exchange of information;
- to revise specific laws dealing with modalities of collection, exchange or management of information in such a way that they are made to conform with the principles.

The first mentioned Law also establishes the need for advance authorization by an independent committee appointed by Parliament of every transmission of personal information by a social security office, and an advance check for compliance with the authorization of each transmission of personal information by a social security office

[19] Belgian Official Journal, 22 February 1990. A co-ordinated electronic French version of this law can be found on http://www.ksz.fgov.be/fr/Legislation/19900115.htm
[20] Belgian Official Journal, 6 March 2002.

by the Crossroads Bank for Social Security. The Crossroads Bank for Social Security also has a legal duty to develop the necessary functional and technical operability framework.

On the basis of this model, independent sector committees with an identical task are being put in place in other government sectors. In order to ensure the necessary co-ordination, all controlling committees will be sector committees of the more general Commission for the Protection of Privacy. Each sector committee will be chaired by a member of the Commission for the Protection of Privacy and will be made up of Commission members on the one hand, and independent experts in the relevant sector, appointed by Parliament, on the other.

7.2. Sufficiently consistent concept definitions

Lawyers are told during their training that each regulatory text has to start with clear definitions of the concepts used within that regulation. If concepts are not defined explicitly, they are interpreted following the commonly used meaning of those concepts. Of course, clear definitions of concepts are necessary. But a problem occurs when several regulatory texts define the same concept in different ways. Typically, government bodies asking for information from citizens or companies by following those concepts will work out instructions in which they explain the concepts, but the task of making the reality fit legal concepts is left to the person who has to provide the information. When confronted with applications for information from several government bodies, applying several regulatory texts that define the same concepts in different ways, the poor citizen or company that has to deliver the information has to describe the same reality using differing concepts.

This evil can be avoided by applying some sane principles to the regulatory process. Legal definitions may continue to vary, but these definitions should refer to information elements and attributes defined during the above mentioned information modelling process. Lawyers can produce as many definitions as they like, but their definitions have to be composed of references to information elements that are defined in the information model. If a necessary information element has not yet been defined within the information model, it will be done, but in a way that complies with the above mentioned information modelling principles.

In so doing, citizens and companies no longer have to interpret the same reality depending on different legal definitions. They only have to supply information in accordance with the information model. The various government bodies can use this information to apply the rules.

It will be clear that the compliance with these principles requires great discipline by everyone involved in working out regulatory texts, also the availability of a thoroughly documented information model. Most constitutional States have an official body that checks the quality of regulations before they are issued. That body could play an important role in implementing the proposed principles.

The vision we described has been implemented in an effective way within the Belgian social security sector for some concepts such as residence, income, working days,

days assimilated to working days, reference periods, … which were previously defined in very different ways across the various social security sectors.

The following methodology has been applied to do this:

- inventory of all documents (frequently) used for information collection;
- inventory of information collected;
- classification of information collected, using cluster methodology;
- breaking the information collected down into 'real life' information elements with descriptions of the attributes requested;
- analysis of goals: what is every 'real life' information element or attribute used for ?
- setting up simplification proposals (e.g. elimination of senseless different treatments of the same 'real life' information elements);
- based on the simplification proposals, fleshing out an object-oriented information model of information to be collected;
- legislation revisions in order to introduce standardized definitions of information elements and attributes, also definitions of legal concepts that refer only to information elements and attributes that are being defined;
- procedures to ensure consistency of the object-oriented information model in an ever changing legal environment.

7.3. Adequate ICT-law

E-government and, in general, the trend towards general use of ICT requires adequate regulation of aspects such as human rights protection with regard to the processing of personal information, protection against ICT crime, ICT security, probative value of electronic information, electronic signatures, equal access to public services, transparency of administration, … In a globalized world, where many processes aren't confined to one country's territory, many of these rules need to be co-ordinated internationally. However, each country has an obligation to implement the principles established internationally into its own legal system.

The European Union has been quite active in working out co-ordinated rules in a set of domains mentioned above. Generally, this is done by promulgating directives. The following directives are relevant in this respect:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[21];
- Directive 97/66/EC of the European Parliament and Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector[22];
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures[23];
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)[24];

[21] Official Journal L 281, 23 November 1995, p. 31.
[22] Official Journal L 24, 30 January 1998, p. 1.
[23] Official Journal L 13, 19 January 2000, p. 12.
[24] Official Journal L 178, 17 July 2000, p. 1.

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[25].

In the areas where European Directives have been devised, Belgium got used to converting them into national law with legislation, the text of which is very close to that of the Directives themselves. This happened, among other cases, with

- the Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data[26], greatly revised by the Law of 11 December 1998 converting Directive 95/46/EC[27], and the royal decree of 13 February 2001 enforcing the Law of 8 December 1992[28];
- the Law of 30 June 1994 on the protection of private life against phone-tapping, introduction to and registration of private communication and telecommunication[29];
- the Law of 20 October 2000 on the introduction of the use of telecommunications methods and of the electronic signatures in legal and non-legal procedures[30];
- the Law of 9 July 2001 setting some rules with regard to the legal framework for electronic signatures and certification services[31].

In the areas where no European Directives have been issued, Belgium has worked out its own national regulations. This occurred for example in the Law of 11 April 1994 regarding administration publicity[32] and the Law of 28 November concerning ICT crime[33].

In general, one can say that Belgian ICT regulations are sufficiently comprehensive and mature to make E-government possible with legal certainty.

For a good overview of the ICT law in force in Belgium, the reader is referred to the handbook *Informatica- en telecommunicatierecht* by Prof. Dr. J. Dumortier[34].

[25] Official Journal L 201, 31 July 2002, p. 37.
[26] Belgian Official Journal, 18 March 1993, p. 5801.
[27] Belgian Official Journal, 3 February 1999, p. 3049.
[28] Belgian Official Journal, 13 March 2001, p. 7839.
[29] Belgian Official Journal, 24 January 1995, p. 1542.
[30] Belgian Official Journal, 22 December 2000, p. 42968.
[31] Belgian Official Journal, 29 September 2001, p. 33070.
[32] Belgian Official Journal, 30 June 1994, p. 17662.
[33] Belgian Official Journal, 3 February 2001, p. 2909.
[34] DUMORTIER, J., *Informatica- en communicatierecht*, Leuven, Acco, 2002, 187 p.

8. Adequate measures to prevent a digital divide

8.1. Introduction

The drawback of integrated services with considerable added value is the danger that a digital divide will open between those who have access to, and are capable of using electronic services and those who don't have access or are not competent at making use of electronic services. It is not just about having access to powerful computers and rapid internet services or not. It is also about people who are latecomers for socio-cultural reasons and have difficulty participating in the electronic society.

For the moment, one can merely note that only a minority of the population is ready for electronic communication. But one can predict with certainty that the change will be as quick as a flash. Both aspects should be taken into account properly.

New research already shows that use of the Internet among low-income people increases less rapidly than among high-income people. Fortunately, developments in the U.S. also show that the time-lags among vulnerable groups with regard to use of the Internet are beginning to decline. Moreover, today, market prices are lower, enabling low-income people to hook themselves up to the electronic superhighway.

However, today the market still does not sufficiently provide for access support for everyone when it comes to ICT skills. This applies particularly the long-term unemployed, the disabled, children of poor parents, the elderly and the homeless. On this point, we need to be vigilant.

8.2. Adequate measures

Measures need to be taken at several levels. A first way for the government to avoid a digital divide with regard to its services is to provide as many services as possible on its own initiative, and thus not allow service delivery to be dependent on an (electronic) application at the customer. This can be achieved by gearing all processes of the various government services to each other, so that information available in the government as a whole can be used to automate the granting of entitlements, or to search actively for low take-up of particular entitlements.

Moreover, and certainly for the citizens, electronic services have to be considered at the first stage as an additional method of service delivery running alongside the traditional methods. The current, 'analogue' form of services must be further supported. E-government can and may only be seen as an extra communication channel between the government on the one hand and citizens and companies on the other. Traditional communication channels such as service counters at the various public offices and intermediaries must continue to deliver services. Moreover, all services must be delivered in the same effective and efficient way, otherwise unjustifiable discrepancies will arise in the treatment of citizens. This implies investment in profound process re-engineering, regardless of the channel through which the citizen calls on the process. Finally, the cost per transaction for citizens and/or companies must on no account vary depending on the method of communication. For the client, then, an E-government transaction must cost the same as a traditional transaction, and the converse. In this way, equal treatment remains guaranteed.

In the meantime, attention must be paid to other, alternative communication channels such as public kiosks, user-friendly terminals, etc., to reach as large an audience as possible, and to permanent education of the citizens.

9. Conclusion

In the first chapter we stated that E-government is a structural reform process that implies a fundamental, customer-oriented re-engineering of the service delivery processes of government bodies as well as organizational changes within those bodies, an interoperability and security framework, co-operation between government levels and government bodies, adaptation of the law, education of customers, measures to prevent a digital divide, … In the other chapters we gave an overview of each of these preconditions for effective implementation of E-government. To conclude, we list a number of critical factors for a successful development of E-government and a number of specific risks that need to be managed.

As critical success factors can be mentioned:

- access to and support of policymakers at the highest level: strong political leadership is crucial to make possible the necessary changes and to guarantee a co-operation between all government levels and government bodies;
- a combination of a long term vision, profound re-engineering and quick wins: political leaders have to be convinced that E-government has to be based on a long term vision and a profound re-engineering of service delivery to the customers; quick wins are useful to prove the interest of E-government and to motivate civil servants to change, but they have to fit with the long term vision; a race for quick wins doesn't stimulate development of well conceived systems based on re-engineering;
- a radical cultural change within government, e.g.
  - from hierarchy to participation and team work;
  - meeting the needs of the customer, not the government;
  - empowering rather than serving,
  - rewarding entrepreneurship within government ;
  - ex post evaluation on output, not ex ante control of every input;
- the creation of service integrators at each government level that co-operate to propose a common vision and that stimulate and co-ordinate the E-government initiatives.

Among other things, risks have to be managed especially concerning:

- security and privacy protection;
- the fact that an average public sector project is more complex than an average private sector project, due to
  - interaction with a larger number of stakeholders (elected officials, civil servants, members of interest groups, voters, tax payers, recipients of public services, other governmental bodies, other government levels, …);
  - execution in a less stable environment, due to regular changes of the policymakers;
- public sector tends, perhaps for reason of prestige, to favour tailor-made, high-risk, state-of-the-art solutions even when alternative, off-the-shelf, cheap, tried and tested systems are available;
- in the public sector, there is typically no financial margin of value to be added by innovation;
- intermediaries often perceive e-government as a threat;
- lack of skills and knowledge.

List of abbreviations

24/7: 24 hours a day, 7 days a week
ASP: Application Service Provider
CA: Certification Authority
CBSS: Crossroads Bank for Social Security
CPS: Community Public Service
DB: DataBase
DS: Directory Service
EDI: Electronic Data Interchange
ERP: Enterprise Resource Planning
FEDICT: Federal Public Service Information and Communication Technology
FPS: Federal Public Service
FTP: File Transfer Protocol
HTML: HyperText Markup Language
HTTP: HyperText Transfer Protocol
ICT: Information and Communication Technology
ISO: International Organization for Standardization
ITIL: Information Technology Infrastructure Library
LDAP: Lightweight Directory Access Protocol
MAN: Metropolitan Area Network
OCSP: Online Certificate Status Protocol
PC: Personal Computer
PDA: Personal Digital Assistant
PDF: Portable Document Format
PIN: Personal Identification Number
PKI: Public Key Infrastructure
PUK: Personal Unblock Key
RA: Registration Authority
RPS: Regional Public Service
SIS(card): Social Identification System
SLA: Service Level Agreement
SMTP: Simple Mail Transfer Protocol
S/MIME: Secure/Multipurpose Internet Mail Extensions
SOAP: Simple Object Access Protocol
SSL: Secure Sockets Layer
SSO: Social Security Office
TCP/IP: Transmission Control Protocol/Internet Protocol
UDDI: Universal Description, Discovery and Integration
UML: Unified Modelling Language
VAT: Value Added Tax
WSDL: Web Services Description Language
XML: eXtensible Markup Language
XSL: eXtensible Stylesheet Language