eServices in the Belgian social sector: a successful combination of business process re-engineering and computerization

Frank Robben

General Manager

Crossroads Bank for Social Security

1. Introduction

In the mid eighties, I started a research programme at the Institute of Social Law of K.U. Leuven under the direction of (amongst others) Prof. Dr. Jef Van Langendonck on the possibilities the use of information and communication technology could offer to improve the social policy making and the functioning of social security.

Based on the results of this research, a major business process re-engineering and computerization was carried out during the past twenty years by about 2,000 Belgian actors in the social sector. Their close collaboration led to the implementation of a network for electronic information exchange which includes public and private institutions from different levels (national, regional and local). An integrated electronic work flow has consequently been developed between companies and social security institutions. A social security portal is available containing integrated services (information and transactions). The portal is intended for citizens, companies and social workers.

The actual eServices in the Belgian social sector demonstrate the results of a strategic information management plan based upon common basic principles and the use of common tools for data sharing and exchange. In October 2002, the Belgian social sector case was mentioned as best practice in the web-based survey on electronic public services ordered by the European Commission. During the second Conference on eGovernment in Como in July 2003, the global eService project of the Belgian social sector was nominated in the category ‘European, Central and Local Government eCo-operation and Public eServices’ as one of five ‘best practices’, selected from some 500 valuable projects. In December 2004, the Crossroads Bank for Social Security received the Belgian eGovernment Champion Award for the quality of its results, both in back office integration and improvement of front office service delivery. At the same time, the Belgian social security institutions received a Belgian eGovernment Award for an improved service delivery to the companies.

This article briefly describes the basic principles applied to rationalize information management in the Belgian social sector (and the Belgian public sector in general), the results obtained in the social sector and, as a conclusion, a number of critical factors for a successful development of eGovernment and a number of specific risks that need to be managed. More detailed information on these topics can be found on my personal website available on http://www.law.kuleuven.ac.be/icri/frobben/

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 into account information about the living circumstances of the beneficiaries and their direct environment, and so forth.

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. 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 definition 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 (for example the residence on 1 January of a given year) or to a situation during a period (for example 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 Unified Modelling Language (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, and so forth).

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 the quality of information.

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 (for example 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, a body requiring information or a service integrator.

Electronic information exchanges should take place on the basis of a 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 designated by Parliament, 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.

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. eService in the Belgian social sector

The 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 assistance schemes (allowances for the disabled, guaranteed family allowance, minimum income and guaranteed income 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 230,000 employers have very frequent contacts with those offices to claim their entitlements, provide information, and pay their contributions. On top of that, a huge number of public and private institutions grant supplementary benefits (e.g. tax reductions or exemptions, free public transport passes, …) to citizens based on their social security statute.

At the time, an in-depth analysis of the functioning of social sector 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, information was requested 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 from another social security office or government body 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. New, integrated and ICT-based processes have been implemented. 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 member 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 member of his staff has performed, 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 and historic work or equivalent performance no longer has to be reported as it is obtained from the quarterly declarations of income and working time data; only if income and working time data are necessary

    concerning a period for which the quarterly declaration has yet to be made, will the income and working time data for this period still need to be reported in the form of a 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 members 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 income 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; every 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;
- a task sharing has been implemented between all social security offices with regard to information storage, information management and information validation;
- all social security offices have the obligation to report suspected information inaccuracies to the office that has been designated to validate that information;
- all social security offices are connected to 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:

- hundreds of types of paper documents which socially insured persons or their employers had to request at one social security office or government body and had to pass to another social security office have been abolished and replaced by 181 types of electronic messages that are exchanged directly between the social security offices and government bodies in question; in 2004, 378.3 million concrete electronic data exchanges took place;
- about 50 types of social security declaration forms have been abolished;
- in the remaining social security declaration forms the number of headings has been reduced on average to a third of the previous number;
- many declarations made by the employers are created and transmitted directly and electronically by employers' staff administration and accountancy software; employers can use at the present time 27 operational electronic transactions;
- in 2004, 13.4 million concrete electronic declarations were carried out by the employers;
- 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 offices 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 the employer and the employee/civil servant (entering service, performing work, falling sick, leaving the company, becoming unemployed, retirement, and so forth);
- personal services to socially insured persons and employers are provided;
- many supplementary benefits are granted using automated procedures, without the socially insured persons or their employers needing to make declarations anymore.

4. Conclusion

From our experience can be deducted a number of critical factors for a successful development of eGovernment 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 process re-engineering and quick wins: political leaders have to be convinced that eGovernment 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 eGovernment 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, for example
  - from hierarchy to participation and team work;
  - meeting the needs of the customer, not of 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 eGovernment initiatives.

The following risks have to be managed

- insufficient security and privacy protection measures;
- 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, and so forth);
  - execution in a less stable environment, due to regular changes of the policymakers;
- the fact that the 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;
- the lack, in the public sector, of sufficient financial means for innovation;
- the fact that intermediaries often perceive eGovernment as a threat;
- the lack of skills and knowledge.

5. References

Robben, F. and Deprest, J. (2003). *E-government: the approach of the Belgian federal administration*. Brussels, Crossroads Bank for Social Security & FEDICT, 55 p. (see http://www.law.kuleuven.ac.be/icri/frobben/publication%20list.htm)

The personal website of Frank Robben is available on http://www.law.kuleuven.ac.be/icri/frobben/

The website of the Crossroads Bank for Social Security is available on http://www.ksz.fgov.be

6. List of abbreviations

eGovernment: electronic government
eServices: electronic services
ICT: Information and Communication Technology
UML: Unified Modelling Language
XML: eXtended Mark-up Language