User and Access Management in Belgian e-Government

Jos Dumortier - Frank Robben

Interdisciplinary Centre for Law and ICT (ICRI), K.U.Leuven
Sint-Michielsstraat 6, B 3443
BE - 3000 LEUVEN

jos.dumortier@law.kuleuven.be
frank.robben@ksz.fgov.be

Abstract

Efficient e-government is not possible without integrated information management. From a privacy protection perspective systems integration has to be preferred over data integration. A well-accepted model for the organisation of user and access management in this perspective is a federation based on circles of trust. The following pages describe how this model is implemented in Belgium, using five building blocks: unique identification numbers, the electronic identity card, validated authentic sources, service integrators and sector committees for data protection. Using these building blocks user and access management is organised following a generic policy decision model. The objective is to illustrate that integrated e-government is not necessarily incompatible with optimal protection of privacy.

1 E-Government Requires Integration

Information management in the context of e-government has to ensure that the government can provide effective services to citizens, companies and other organisations. This is not possible without far-reaching integration. Citizens and companies assume that the government as a whole will only request the necessary information once and, after checking for accuracy, will then reuse the information whenever it needs to do so. With this in mind, agreements must be reached between government echelons and agencies. Which agencies gather which information, check it for accuracy, store it and make it available for other echelons and agencies?

Everyone expects services from the government aligned to specific situations and also offered as far as possible in personalised form.[1] The alignment of services to specific situations can be achieved by offering services from the perspective of the user. Citizens and companies no longer have to find their own way through the labyrinth of government institutions and competences, but receive integrated services relating to events taking place throughout their lives: birth, work, housing, illness, retirement, death, starting a business, etc. However, this presupposes that these services are offered across all government echelons, government agencies and private bodies.

[1] The Belgian OECD report on e-Government (2008) reads (p. 19): "Belgian citizens are more interested in accessing relevant, personalised services online, rather than learning the complexities of Belgian governments' competences". The full study is available from http://www.fedict.belgium.be/nl/downloads/.

Citizens, companies and their service providers must be able to find all the relevant information and services using one electronic access portal of their choice. This electronic access portal must not be unique in the sense that there can only be one, but users must be able to find everything they want regarding a given event on the electronic access portal of their choice. This requires that electronic services from different government echelons and agencies can easily be integrated into electronic access portals by all those who develop them.

Automation today is generally being developed by governments according to a Service Oriented Architecture (SOA). SOA is essentially an architecture for distributed development, management and use of ICT components, which call upon each other as services. It allows all those involved in electronic government service delivery to work together but still to maintain their individual autonomy and specific working methods. Local administrations and associations, health insurance funds, trade unions, banks, accountants, employment agencies, etc., can integrate the electronic services provided by the government – whether or not supplemented by their own services – and then offer them in a manner that is ideally suited to their target group. Companies or other end users can also have their internal company applications interact directly with electronic government services.

Where possible, users want services to be provided automatically. The government can, for example, relieve them of the burden of applying for tax deductions or exemptions, reduced rates for utility services, free public transport or other benefits that are allocated to them based on a social situation previously known to the government. At the same time, however, active contribution and a high level of self-service and self-steering are also appreciated. Services have to be offered in an efficient and user-friendly way, through various channels depending on the user's choice, as well as being reliably, securely and permanently available.

Government policy is expected to be based on objective and updated data. Citizens rightly demand that the government takes a proactive stance and that policy anticipates new trends. Everyone also wants the government to combat all forms of fraud in an efficient manner and to apply the most modern data mining techniques to do so.

All these requirements have to be reconciled with maximum protection of privacy. Of course, that does not happen automatically. In the quest for efficiency, it is easy to fall into the trap of a higher level of data concentration and centralised processing.

The Belgian approach demonstrates how the latter can be avoided, in particular by implementing a federated user and access management. Below we broadly describe how this approach has been conceived in Belgium.

2 Definitions

User and access management consists, as the term itself indicates, of two parts: user management and access management. User management itself covers five aspects: 1) identity registration, 2) user identification, 3) identity authentication, 4) registration of attributes and mandates and 5) verification of attributes and mandates. Access management covers the registration of authorisations and the verification of authorisations.

Within the context of this paper, the following definitions of the above terms are used: [2]

- The *identity* of the user is a unique number or a series of attributes of a user (natural person, company, branch of a company, etc.) enabling the user to be unequivocally identified. This implies that a user has one and only one identity. The fact that a pseudonym can be used in certain situations does not alter this fact.

[2] These definitions are also used by the Belgian Privacy Commission in a Recommendation regarding access and user management in the public sector (SE/2008/028) of 24 September 2008 (www.privacycommission.be)

- An *attribute* is any user characteristic, other than the attributes that determine the identity of the user, such as a specific quality, a position in a certain organisation, a professional qualification, etc. A user can have several attributes.
- A *mandate* is a right granted by an identified user to another identified user to perform a number of well-defined (legal) transactions in his name and on his behalf. A user can grant one or more mandates to one or more users.
- *Registration* is the process used to establish the identity of a user, a user attribute or a mandate with sufficient certainty before resources are made available and that is used to authenticate or verify an identity, an attribute or a mandate.
- *Authentication* of identity is the process of checking that the identity a user claims to hold does indeed belong to him. This can be carried out by checking: a) knowledge (e.g. a password), b) possession (e.g. a certificate on an electronically readable card), c) (a) biometric trait(s), or d) a combination of two or more of these means.
- *Verification of* an attribute or a mandate is the process of checking whether an attribute or a mandate that a user claims to have in order to be able to use an electronic service is actually a characteristic or mandate of this particular user. This can be carried out: a) based on the same type of means as those used for identity authentication, or b) after authentication of a user's identity, by consulting a database (authentic source) in which characteristics or mandates regarding an identified user are stored.
- *Authorisation* is the permission for a user to perform a certain transaction or to use a certain service.

3 Federated user and access management

Theoretically, it would be possible to achieve the objectives of e-government information management outlined in the introduction by centralising all the data concerning natural persons, legal persons and other entities as much as possible. Some years ago, there was a discussion in the Netherlands about a proposal to create a "digital vault" for every citizen. This would be controlled by the data subject and would combine all the data about this data subject that need to be available for use by the government. Ultimately, this idea was abandoned because of privacy and security concerns.

For this reason data protection supervisory authorities are often of the opinion that e-government data exchange should be organised as far as possible based on a distributed and decentralised storage of personal data.[3] A model that is frequently used for this purpose by the private sector is the model of a federation based on circles of trust.[4] Such a model implies that clear agreements are reached among the bodies involved in the electronic service delivery in order to organise user and access management together. Among other things, these agreements establish who performs which authentication, verification and checks, using which means, and who is responsible and liable for them. Agreements are also needed to determine how the results of the authentications, verifications and checks performed can be electronically exchanged in a secure way between the relevant bodies. Who maintains which log files and how is it possible to ensure that an investigation – on the initiative of an inspection body or fol-

[3] In its Working Document on Online Authentication Systems, adopted on 29/01/2003 (WP 68) the Article 29 Working Party writes (p.15): „The adoption of software architecture that minimises the centralisation of personal data of the Internet users would be appreciated and encouraged as a means of increasing the fault-tolerance properties of the authentication system, and of avoiding the creation of high added-value databases owned and managed by a single company or by a small set of companies and organisations."

[4] The model is based on the results of the "Liberty Alliance" project: http://www.projectliberty.org/.

lowing a complaint – can perfectly reconstruct who has used which service for which transaction involving which citizen or company, when, via which channel and for what purposes?

Data protection supervisory authorities have emphasised that a federated system avoids unnecessary centralisation and the associated threats to privacy. For example, no copies of the validated authentic sources will be circulated. Moreover, multiple identical checks and the redundant storage of log data are avoided. Furthermore, this model also guarantees that every administration is working with the most up-to-date information. For example, if a user loses a characteristic, this will be dealt with in an appropriate way by the system at the time of registration. Finally, the system will liberate users from repeatedly having to provide proof of the same attributes or mandates.

A federated approach however assumes that everyone is singing from the same hymn sheet, so that all the components fit perfectly together. This is important, because administrative processes take place through various government echelons, institutions and agencies. For this reason, the same building blocks must be used everywhere.

4 Main Building Blocks

The most important building blocks used in Belgium in user and access management for e-government are the unique identification numbers, the electronic identity card, validated authentic sources, service integrators and sector committees for data protection. Each of these five building blocks will be briefly discussed below.

4.1 Unique Identifiers

In Belgium, unique identification numbers are used for natural persons and other entities (companies, associations, etc.) throughout the entire e-government data flow, at all levels and by all government institutions and agencies. Belgian citizens and foreigners living in Belgium are identified by their National Number. For other persons, not living in Belgium but who have contact with the Belgian authorities, the Social Security Identification Number (SSIN) is used. Legal persons and other entities are identified by the company number under which the entity is registered with the Enterprise Register (the so-called "Crossroads Bank for Enterprises").

Sector-specific identification numbers – sometimes presented as more privacy-friendly - are not used in Belgium. There has been some hesitation about using sector-specific identification numbers in the health sector and in field of e-justice, but this idea has finally been abandoned. The Belgian Privacy Commission has explicitly expressed its support to the decision to make use of the National Number (or the SSIN) instead of using a specific patient number in the health sector.

Many applications exceed the boundaries of one particular public sector domain. Working with sector-specific identification numbers can therefore lead to considerable complexity. Experiences in Austria, where sector numbers are used, demonstrate that in practice organisations tend to avoid separate identification numbers in order to work more rapidly and more securely.

The protection of privacy when using unique identification numbers can be guaranteed in various other ways. Use of the number can be restricted or recourse can be sought to strict control on the exchange of personal data that are linked to the unique number.[5] Belgium has opted for a combination of both of these methods.

[5] The Hungarian Constitutional Court (http://www.ceecprivacy.org/htm/91-15.htm) aptly formulated this alternative as follows: "(...) the use of PINs (Personal Identification Numbers) shall be restricted by security regulations. This can be done in two ways: either the use of the PINs is to be restricted to precisely defined data-processing operations or strict conditions or controlling measures are to be imposed on the availability of information connected to PINs and on the link-up of record-keeping systems using PINs".

4.2 Electronic Identity Card

The preferred method of electronic identity authentication in Belgium is the use of an electronic identity card (EID). However, depending on the required security level, use is also made of either a combination of user name, password and citizen token[6], or a combination of user name and password alone. The EID does, however, offer a range of advantages. It combines possession of a specific document with the availability of particular knowledge (PIN code). In addition, a number of factual and legal factors limit the risk of abuse in the event of possible loss or theft of the card.[7]

Verification of the attributes and/or mandates is not performed using the EID. In addition to a device for creating a qualified electronic signature, the EID is exclusively an instrument for identification and authentication. The information on the card therefore remains confined to the data that are necessary to identify the holder, the certificate that allows the holder to authenticate himself and the certificate that enables the holder to place a secure electronic signature. Data that have nothing to do with the identification or authentication of a physical person or the electronic signature, such as characteristics and/or mandates, do not belong on the EID.[8]

4.3 Validated Authentic Sources

The fact that the identity of a user has been authenticated is not always enough to grant the person concerned automatic access to an electronic service. A user's access rights to an electronic service (authorisation) can be linked to his attributes and/or mandates. Integrated user and access management therefore requires that unambiguous checks can be performed on the relevant attributes of a person or the existence of a mandate given by a legal person or a natural person to which an electronic service relates and the person who is using this service.

The verification of attributes and/or mandates (for example, is the user a qualified physician? Is the user a lawful representative of the legal person?) takes place via channels other than the EID. In this context it is not recommendable to rely on non-validated information that is simply provided by the user himself. These elements have to be checked against a source that offers the required guarantees in terms of accuracy and up datedness of the information it contains. In Belgium such sources are called "validated authentic sources". The government agency in charge of a validated authentic source is responsible for the availability and quality of the information it contains and made available for other agencies and echelons. The State Health Insurance Fund, for example, will be in charge of a validated authentic source of qualified physicians, the Royal Federation of Notaries will keep the validated authentic source of notaries, etc.

The extent to which feedback is possible to validated authentic sources is a crucial factor in the success of a reliable electronic user and access management. It is therefore obvious that anyone wishing to expand this type of management system has to know on which sources they can rely. This requires the availability of an inventory of validated authentic sources. For this reason, at every level, government and related services must be identified that provide reliable information with regard to, for example, attributes or mandates of a person. The authentic information must be mapped out and the elements that demonstrate its quality must be indicated. Finally, a validated authentic source is only useful if the information is organised in such a way that it can be easily retrieved.

---

[6] A citizen token is a card (with the same dimensions as a credit card) that contains 24 numbered personal codes and that is sent to the person in question by post following verification of certain credentials (National Registration Number, SIS (social insurance number) card number and identity card number). When access to an application is requested (e.g. Tax-on-Web), the user is asked for one of the codes at random.

[7] Danny De Cock, Christopher Wolf and Bart Preneel, The Belgian Electronic Identity Card (Overview), http://www.cosic.esat.kuleuven.be/publications/article-769.pdf

[8] The Belgian Privacy Commission issued an opinion (no. 1/2005 of 7 September 2005) arguing against the inclusion of aspects such as blood group or the consent for organ donation on the electronic identity card.

4.4 Service Integrators

Integration does not happen spontaneously. Process optimisation that transcends services, coordination of back offices, an integrated and personalised range of electronic services in the front office, coordination of semantics, interoperable electronic platforms developed according to a service-oriented architecture and reliable security and protection of privacy demand close, multidisciplinary cooperation among the various government echelons and agencies. This cooperation is needed in various fields: at the level of vision and strategy building, process re-engineering, the development of information and communication technology, the implementation of the measures regarding information security, the organisation of the required electronic data exchange, the adjustment of legislation, project management, services management, etc.. Moreover, within every government echelon and sector, the required level of consistency must be guaranteed among all these fields.

In various government sectors or echelons in Belgium, bodies have already been successfully designated for this purpose. They are the driving forces behind cooperation and coordination at the aforementioned levels in the relevant sectors or echelons. In this respect, they are responsible for organising the required electronic data exchange and act as "trusted third party", monitoring the correct application of the legislation regarding information security and privacy protection and the exchange of personal data performed within that context. These bodies are known as "crossroads banks" or, better and more up to date, "service integrators".

Examples of already existing service integrators include the Crossroads Bank for Social Security (CBSS) in the social sector[9], the Flemish eGovernment Coordination Unit (CORVE) [10] in Flanders, Easi-Wal[11] in Wallonia and the eHealth-Platform[12] in the health sector.

Service integration has to be distinguished from data integration. The latter involves merging data from various authentic sources and their storage in an integrated database, with a view to their communication to third parties. By contrast, service integration refers to integrating electronic sub-services into integrated electronic services with a view to offering them to third parties. Service integration is also not the same as infrastructure integration (the pure use of a shared infrastructure for separate data processing operations) or presentation integration (purely making data or services accessible in an integrated manner via one electronic point of contact, such as a portal).

When processing personal data, data integration is only acceptable if this is necessary and if the same functionality *cannot* reasonably be provided via service integration. This is a consequence of the proportionality rule. Personal data must not be pooled if this is not necessary for the intended objective. In other words, where service integration offers a solution, it should be given preference.

Ideally, at least if justified by the volume and level of complexity, a service integrator should be designated (such as health, social security, justice or finance) within each government echelon and sector. In the sectors of the federal administration for which an individual service integrator is not justified – for example because the sector is too small - a federal government service for ICT (called FEDICT) takes over. FEDICT act as a service integrator for all government sectors that don't have their own service integrator. In addition, a service integrator exists in each of the three regions: Flanders, Wallonia and Brussels.

The sphere of activity and the tasks of each service integrator is laid down in a legal text. In this respect, a clear demarcation of the fields of application among service integrators is of the utmost importance. A vague demarcation of the sphere of activity of the different service integrators would lead to undesirable competition among service integrators in the public sector. Every service integrator further

---

[9] http://www.ksz-bcss.fgov.be/Nl/index.asp

[10] http://www.corve.be/

[11] http://easi.wallonie.be/xml/

[12] https://www.ehealth.fgov.be/nl/homepage/index.html

acts under the control of a Sector Committee of the Privacy Commission. This Sector Committee authorises service integration after testing it against the principles of the data protection legislation.

Experience with service integration has also demonstrated that every service integrator can best be managed by representatives of the various stakeholders in the relevant sector. In addition, the persons involved (patients, tax payers, etc.) must also be represented. This is important not only to enjoy the necessary trust, but also to guarantee a user-oriented operation. The service integrator may on no account detract from the responsibility and autonomy of the federal or regional government agencies themselves.

Explicit care is taken to ensure that each (federal) government agency only falls within the coordination of one service integrator. As a result, for each government agency, a coordination unit and the necessary link to only one electronic data exchange platform is ensured and a different approach to the same government agency by various service integrators is avoided. The various service integrators must ensure, in a consultation platform, the necessary mutual coordination and interoperability so that the various government agencies served by each of them can also use the electronic services of government agencies that are served by another service integrator. For example, in order to grant study allowances, the ministry of education will need a service from the service integrator of the public finance sector, in order to check the income of the applicant or his parents.

At the level of the ICT architecture, the cooperation model among the service integrators can be represented as follows:[13]

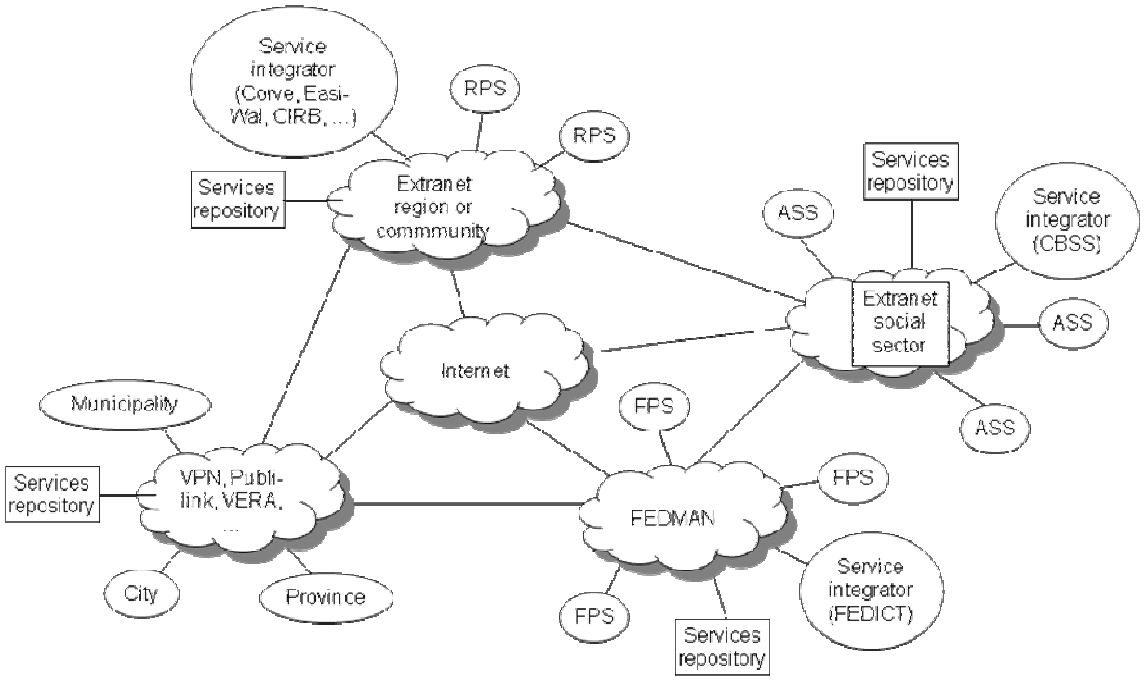

Fig. 1: Service integration architecture in Belgian e-Government

[13] Key: FPS: Federal Public Service
ASS: Agency for Social Security (health insurance fund, employment agency, etc.)
RPS: Regional Public Service
VPN: Virtual Private Network

For each government echelon or sector, the relevant service integrator encourages cooperation at the aforementioned levels and coordinates the development of electronic services within its echelon or sector. The available electronic services are published in a services repository. These electronic services can be called upon by third parties and can be further used as building blocks for their own electronic service delivery.

Every service integrator manages a (virtual) network, and the various networks are linked. In this context, each service integrator acts as an independent trusted party, which does not itself fulfil any substantive tasks regarding data processing or storage and which ensures that the measures regarding information security and privacy protection are applied in practice within the government echelon or sector within which it operates and in the communication of personal data to other service integrators.

One important tool in service integration is the reference repertory. This repertory has a three-fold structure:

- who/where/how/when table (personal repertory): which people hold files in what capacities for which players regarding which periods?
- what/where table (data availability table): which types of personal data are available from which types of actor in the various types of file?
- who-gets-what table (access authorisation table): which personal data can which types of actor obtain regarding the various types of file and regarding which periods? Which personal data are automatically communicated regarding the various types of file and under what circumstances?

For example, the reference repertory of the service integrator in the health sector (the eHealth-Platform) will contain e.g. information on which physician or hospital contains which data with regard to a particular patient, identified by his/her Social Security Identification Number, and who has been granted which rights related to these data. The (medical) data themselves remain in the hands (computers) of the physicians and hospitals involved.

The reference repertory is in particular necessary for routing information, preventive access control and automatic communication of changes. Most importantly it avoids large-scale central storage of personal data.

4.5 Sector Committees for Data Protection

Within the Privacy Commission a number of so-called "Sector Committees have been created.[14] These committees are composed on the one hand of representatives from the Privacy Commission itself and, on the other hand, of independent experts in the relevant fields (e.g. social security, health care, etc.). The members are appointed by the federal or regional Parliament.

The most important task of a Sector Committee is granting authorisations for the (electronic) exchange of personal data, apart from the cases where this is explicitly permitted by law. For example, imagine that a regional public transport company wishes to automatically check whether a person is officially registered as a person with a handicap by the relevant social security institution. In order to obtain these data via a service offered by the service integrator of the social security sector, the regional public transport company will need to apply for an authorisation of the competent Sector Committee. The Committee will examine the application

[14] The Law of 26 March 2003 introduced an Article 31bis into the Belgian law regarding the protection of privacy with respect to the processing of personal data, § 1 of which reads as follows, "Within the Commission, the law creates sector committees that are competent to examine and to assess requests relating to the processing or communication of data to which special legislation applies, within the confines established by the law".

e.g. from a proportionality and security point of view. The authorisation will often include recommendations on how to organise the data exchange in the most privacy-friendly way.

Other tasks include establishing the organisation and policies, providing opinions and recommendations and dealing with complaints regarding infringements. Finally, the Sector Committee also exercises preventive control over the lawfulness of the exchange of personal data by a service integrator.

The authorisations of the Sector Committees are public and are published on the web site of the Privacy Commission. Over the years they constitute a authoritative body of jurisprudence with regard to personal data protection in the domain of e-government.

5 Generic Policy Application Model

How are the building blocks described above actually used for user and access management in the Belgian e-Government context?

The authorisation to use a service is given by the provider of the service, if necessary subject to prior authorisation by the competent Sector Committee. For this purpose, the identity and attributes and/or mandates of the user need to be checked. The authentication of the user's identity takes place - depending on the required security level – by means of the electronic identity card, a combination of user number, password and citizen token or a combination of user number and password. Next, verification of attributes and mandates is carried out via access to one or more validated authentic sources.

Conformity of a specific request for access with access authorisations (does the user, identified as a qualified physician, have access to this patient's file?) is preventively validated by the competent independent service integrator, for instance using the reference repertory. All accesses are electronically logged at the level of the user so that, in the event of complaints, it is possible to check subsequently whether access was legitimate (only who/what/when, not content). Access to the log files is strictly protected.

This is all developed using a generic policy application model that is summarised in the following diagram:

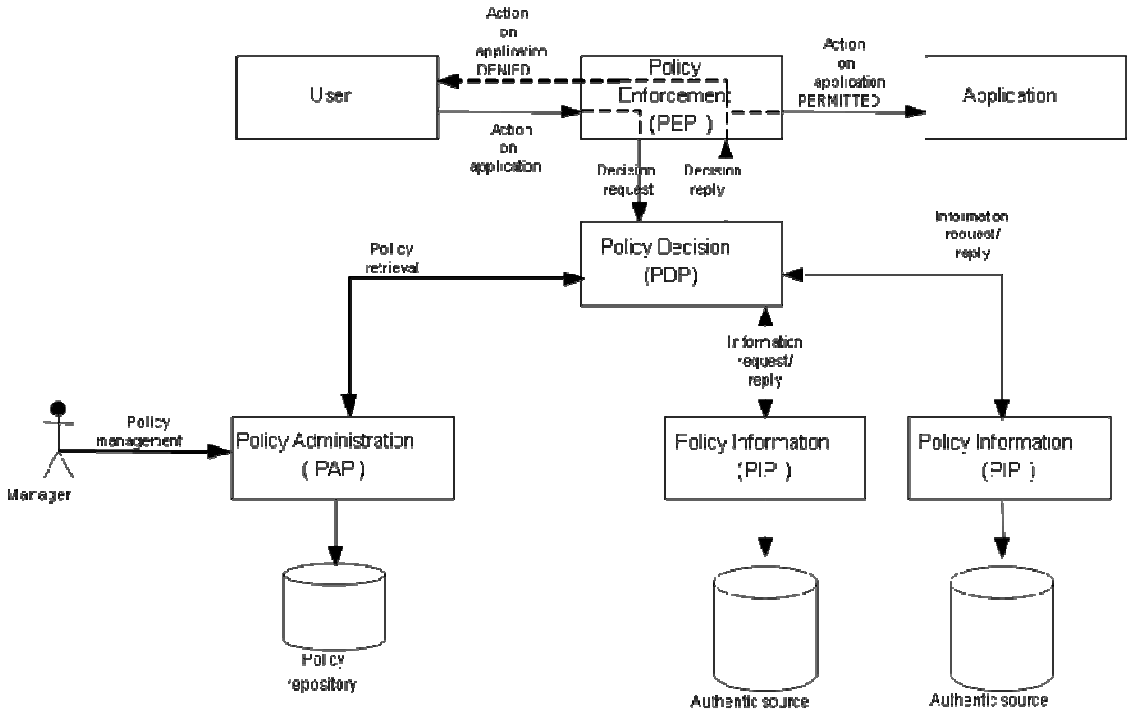

Fig. 2: Generic Policy Application Model

- The process begins with an authorisation request (application action) on behalf of a user. This request reaches the Policy Enforcement Point (PEP), together with all the available information about the user, the requested action, the resources and the environment. Following initial validation, the authorisation request is then forwarded to the Policy Decision Point (PDP) to obtain an authorisation decision (decision request). Based on the response (decision response), access is granted to the application, with forwarding of relevant credentials (application action permitted) or this access is denied (application action denied).
- Based on the authorisation request received, the appropriate authorisation policy is looked up in the Policy Administration Point(s) (PAP). This policy is evaluated and, if necessary, the relevant information for it is retrieved from the policy information point (PIP). Depending on the result, an authorisation decision (permit/deny/not applicable) is taken and forwarded to the PEP.
- The "Policy Administration Point"(PAP) is the environment for storing and managing the authorisation policies by the competent person(s) designated by the party who is responsible for the application. This information is stored in a "policy repository". The PAP ensures that the authorisation policies are made available to the PDP for making a policy decision.
- The function of the PIP (Policy Information Point) is to make information available to the PDP for evaluating the authorisation policies. The information comes from authentic sources with information about qualities, mandates, etc.

6 Conclusion and European Outlook

As in all other Member States of the European Union, user and access management in Belgium is conceived primarily on the basis of persons and entities that are registered in Belgium, whether as Belgians or as foreigners with residence in Belgium. Of course, for persons and entities wishing to use electronic government services for the first time from other countries, user and access management is highly problematic. How can a building contractor in Poland electronically declare the employment of his employees on a Belgian building site using the Belgian social security portal? Or how can an Italian manufacturer of office furniture submit his tender on the Belgian portal for public procurement?[15]

Interoperability is the goal at European level between the systems that are used for user and access management in the Member States.[16] With a view to implementation of the Services Directive and, in particular, the obligation regarding the central electronic help desk which every Member State must provide for, this aspect is also very important.[17] For the time being, Belgium is working with pragmatic solutions. For identity registration, the data are provided by the foreign user. For applications with a lower risk of fraud, such as the declaration of employees to the social security administration, this method is acceptable for the time being.[18] For the future serious efforts are needed to enhance interoperability between the user and access management systems put in place by the European Member States.

Index

e-government – identity management – privacy – personal data protection - Belgium

[15] https://enot.publicprocurement.be/home.do

[16] See http://ec.europa.eu/idabc/en/document/6484/5644

[17] For more details: Report on the State of Pan-European e-ID Initiatives (ENISA), 2008: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_eID_management.pdf

[18] Example: the web site www.limosa.be where foreign employers who employ staff in Belgium can electronically fulfil the obligation to submit a prior declaration of employment to the Belgian social security administration.