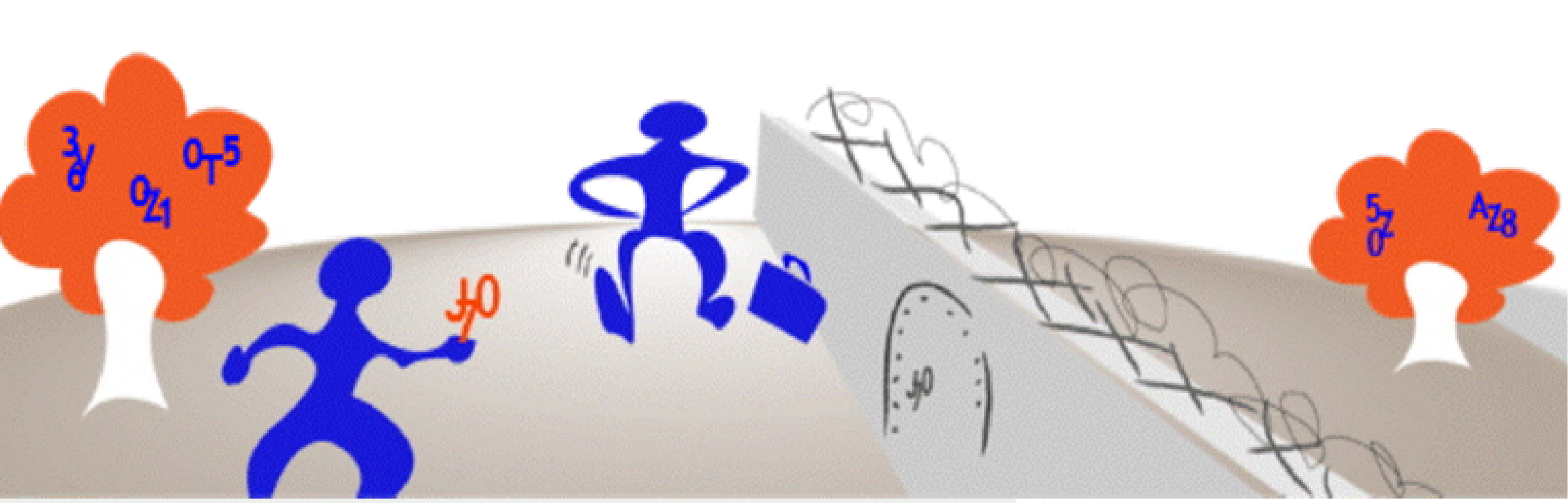
European Journal of ePractice

A publication of epractice.eu

Meet > Share > Learn at www.epracticejournal.eu

Nº 6 · January 2009

Key enablers for eTransformation? eID, Interoperability and Open Source



Editorial

Articles

The European Journal of ePractice is a digital publication on eTransformation by ePractice.eu, a portal created by the European Commission to promote the sharing of good practices in eGovernment, eHealth and eInclusion.

Edited by P.A.U. Education, S.L.

Web: www.epracticejournal.eu
Email: editorial@epractice.eu

Editorial: Key enablers for eTransformation? eID, Interoperability and Open Source

Dr. William H. Dutton

Professor of Internet Studies and director of the Oxford Internet Institute, University of Oxford

The European Commission's eGovernment Action Plan considers innovations in eIdentification, interoperability and open source software to be keys to opening the door to the transformational potential of eGovernment. The developers of eGovernment services are therefore directing additional resources on these innovations as a means for providing high impact services. But will initiatives in these areas work? Will they facilitate the efficient and correct operation of public eServices? What does the evidence suggest?

The contributions to this special issue highlight the challenges confronting efforts to create these enabling conditions. Interoperability and appropriate identification systems are major challenges in their own right. As some contributions argue, open source can help some government agencies approach these goals, but it is only one of many strategies that need to be considered.

Professor Herbert Kubicek and Ralph Cimander point out the multifaceted nature of interoperability. Their analysis of good practice cases argues that the organization conditions for interoperability have been relatively neglected compared to the technical and semantic requirements. They present a useful model that suggests each of these dimensions of interoperability must be addressed from three perspectives simultaneously: politically, to negotiate among institutional actors; functionally, to align data, information and workflows effectively; and as a service to govern and regulate directories, formats, and the routing of messages.

Interoperability is also on focus at the case study of the European Services directive by Christian Breitenstrom and Jens Fromm, who point to the value of open source software (OSS). In their experience, OSS is not only a cost saving mechanism; it can also support communication and thereby help to achieve interoperability. Interoperability is also taken up by Sylvia Archmann and Just Castillo Iglesias, who argue that in order to succeed it requires the sharing of experiences and the development of communities of practice across Europe, key objectives of this journal.

The last two contributions focus on identification as a key to service delivery. The value of open source software is the major theme of Bud P. Bruegger, who concludes that this approach was necessary for the development of an eIdentification access control system, given the limited resources available for their project. He therefore sees open source as a major enabler. In contrast, based on their work in health services, Elena Sini, Paolo Locatelli, Nicola Restifo, and Michele Torresani focus on the use of a smart card and RFId for the integration of patient records and information across institutions.

This diverse set of contributions moves the debate about transformational eGovernment forward, by taking us one step back. They all show that there are no quick fixes to eGovernment. The key enablers themselves are technical, economic and organizational challenges that are intertwined in ways that make it difficult to attack single constraints. Interoperability, identification, open source and other enablers of eGovernment are closely interrelated. Together and separately, they need to be addressed and reconciled with countervailing concerns, such as over privacy and data protection.

European Journal of ePractice

A publication of epractice.eu

Three dimensions of organizational interoperability.
Insights from recent studies for improving interoperability frame-works

Interoperability (IOP) is considered a critical success factor to forge ahead in the online provi-sion of public services. Interoperability frameworks shall give guidance to practitioners what to consider and to do in order to enable seamless interaction with other public authorities and clients. The well known European Interoperability Framework (EIF) and many others are designed as multi-layer models, distinguishing between technical, semantic and organizational IOP. For achieving technical IOP there are acknowledged standards; for semantic IOP recognized concepts and methods are available. However, aspects and characteristics of organizational IOP, although considered to be an important success factor for eGovernment projects, are much more heterogeneous and do not provide similar guidance.

This paper suggests that it will be useful to separate this heterogeneous collection of organizational issues into three dimensions. In line with the assignment of standards and protocols to the technical and semantic layer, an additional layer, presently called organizational IOP, should be confined to standards and concepts dealing with the linkage of business processes and be called business process IOP. All other organizational aspects should be conceived as cross-cutting dimensions, as they refer to elements on all layers.

Relevant characteristics of more than 70 good practice cases have been collected within a Study of IOP for the European Commission. Based on these indicators, an empirical taxonomy of settings for achieving IOP at present is developed within an ongoing research project. The proposed classification is presented here in order to invite comments by the IOP community and at the same time is recommended for the discussion about the new draft of the EIF 2.0, issued in July 2008[1].

Herbert Kubicek

Ralf Cimander

Institute for Informationmanagement Bremen (ifib)

Keywords

E-Government, eGovernment, Organizational Interoperability, Governance, IT-Governance, Integration of Information Systems, Centralization, Standardization, EIF, IOP, interoperability frameworks.

“ These items shall allow the support of the decisions that had to be taken by public authorities in order to provide for and guarantee interoperation and interoperability. “

[1] The EIF v2.0 will take the form of an official Commission position with the publication of a Communication from the Commission to the Council and to the Parliament early 2009.

1 Defining the subject: integration and/or interoperability

There is wide agreement in administrative practice and research that the use of ICT will only lead to savings and improvements if business processes are reorganized in order to allow for a seamless exchange of data between all agencies involved. In many public services, several back-offices are involved in the service-supply-chain. The data processing systems in the back-offices of these agencies have to be merged or linked up in a way to allow for a smooth online service provision across organizational boundaries. However there are legacy systems in these back-offices that do not have the aspired interfaces and are difficult to change because they are linked with other systems and fulfil the local requirements of the respective agency quite well. Reorganization of back-offices cannot start from scratch. There is a need for developing a strategy which may provide a compromise between keeping local systems and still allowing for better data interchange.

In a Study for the European Commission on Back-office Reorganization, about 30 Good Practice Cases have been analyzed and three strategies have been identified. The two basic strategies for coordination, which have been distinguished in organization theory for decades (March & Simon 1958, Kieser & Kubicek 1993), are either centralization of tasks or standardization of processes. As a third intermediate strategy, clearing houses have been identified (Millard et. al. 2004, Kubicek, Millard & Westholm 2007).

In this context, centralization of tasks also means a centralization of data and processing functions, which formerly have been fulfilled separately in different agencies. It requires the physical merging of data from different IT-systems and is also called (data) integration. In the Back-office Reorganization Study it turned out that high savings could be achieved by public services that have realized full or almost full integration of back-offices via centralization. However, as centralization of tasks of formerly separate agencies means changes of authority and jurisdiction, this only happened when there was strong political pressure because of obvious inefficiencies, delays and backlogs.

An alternative option is the standardization of processes. Electronic Data interchange becomes possible if different agencies strictly follow the same procedure and use the same data formats. In the cases of linking IT systems in different agencies in an interorganizational information system, this does not necessarily mean that internal processes, data formats and processing functions have to be standardized, but only the interfaces at the boundaries of each local system and the content and format of the data to be exchanged. Instead of integrating the separate systems into a new one, they can be kept running and only be adapted in order to provide for their interoperation via import and export interfaces. Therefore, we may speak of interoperability via standardization. Scholl & Klischewski (2007) suggest distinguishing between “interoperability” (IOP), as the ability to allow for data exchange, and “interoperation”, as the practical achievement.

In principle, interoperation could be achieved by direct multilateral data exchange according to the same standards by all agencies involved. However, in practice, very often intermediaries are involved, providing certain support such as directory or data conversion services. Of course, all participating agencies could run their own directories with the addresses of all partners. But obviously the cost for updating is lower if this is done only once for all participating units via a central directory. Following the terminology in the banking industry, such intermediaries have been named clearing houses in the Back-office Study. Contrary to the centralization by data integration, where primary tasks and responsibilities for e-services are centralized, the primary tasks and responsibilities remain unchanged and only secondary, supportive functions are centralized by outsourcing them to one or more service providers.

To sum up, efficient electronic public services depending on the cooperation of two or more agencies can either be achieved by centralization of tasks and integration of data or through achieving interoperation by standardization of interfaces and data formats, frequently realized with the help of intermediate agencies called clearing houses providing limited supporting secondary services for achieving interoperation. This means that IOP is one of at least two different strategies to enable high quality and highly efficient eGovernment services across organizational boundaries, which comes on the agenda when centralization of tasks is legally not possible, politically not feasible or not the best option because of other risks.

This basic distinction shall be illustrated by two examples from a study on IOP for the European Commission within the MODINIS program (Tambouris et. al. 2007), where the authors also were involved in. In Austria and in Germany, citizens have to register in the local community where they live. When moving to another local community, they have to deregister in their old community and register in the new one. With the introduction of electronic citizens' registers this did not change for some time. Each local community had ordered their own system. In Germany there are about 5,400 local citizens registers operated on at least 17 different software products. In such a heterogeneous environment, a request of official address information to localize a certain citizen is difficult to fulfil, and obviously there is a double burden by completing two forms with almost identical content in the case of moving. Therefore, projects where launched in both countries to improve the services of address verification and change of address. For several reasons both countries decided to go different ways. In Austria the national government decided to set up a central national citizens' register and committed all local registers to deliver their data or to use the central register, instead of their local one free of charge. In Germany this was not possible at that time because the citizen's registration was in the jurisdiction of the 16 Länder under coordination of the Federal Government, and there were strong privacy concerns. Therefore the Federal Government in Germany decided to use a coordinating authority to establish a standard for data exchange between the local communities and standard procedures for services such as address verification and change of address. This X-Meld standard was finally established in a conference of the 16 state ministers of Interior and the Federal minister and enacted in a directive, which only demands the implementation of an interface of the local or regional system which can receive and send messages according to the X-Meld standard[1].

According to the terminology introduced in this paper, the Austrian case of establishing a central register is not a case of IOP, but of integration, while the German case is a true case of establishing IOP between more than 5,400 local systems by enacting the X-Meld standard for multilateral data exchange.

This understanding of IOP is in line with the definition adopted by the European Commission and the European Interoperability Framework which defines IOP as "the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable sharing of information and knowledge" (IDABC 2004).

2 Basis, objective and outline of this analysis

Both strategies require complex and difficult measures, which may be quite different. This paper will only focus on how IOP has been achieved and is maintained in a number of good practice cases collected in the aforementioned MODINIS IOP Study (Tambouris et. al. 2007, Archmann & Kudlacek 2008). More than 70 case descriptions have been made available in an online database[2]. For 32 of these cases, extensive descriptions have been produced in cooperation with the case owners and been published on the Good Practice Framework for E-Government of the European Commission[3]. Further analysis of these cases is subject of a research grant provided by the German Research Foundation (Deutsche Forschungsgemeinschaft), started in May 2008.

Whereas IOP is mostly treated as a technical issue of developing or selecting the appropriate technical standards, the MODINIS IOP Study also aimed at identifying barriers and success factors of achieving IOP. While, within the available scope of time and funds, the study could only summarize insights from the cases, the research project aims at an empirical taxonomy based on operational indicators. So far, there are neither appropriate analytical nor empirical classifications of different approaches toward establishing and maintaining IOP. But there are IOP frameworks developed to provide some guidance and to classify different problems that arise, when striving for IOP. They mainly concentrate on what has to be made interoperable and by which technical means, i.e. standards, by distinguishing different layers of IOP, e.g. a technical, syntactic, semantic and organizational layer.

Compared to the other IOP layers, the aspects and characteristics of organizational IOP are the less systematized, although regarding to barriers and success factors many experts agree that organizational IOP constitutes the biggest challenge for the successful implementation of interoperable multi-level eGovernment systems (see for example a survey on information needs regarding IOP within the MODINIS IOP Study, Kubicek & Cimander 2005).

[1] see http://www.egov-iop.ifib.de/case_description.php for the two cases

[2] http://www.egov-iop.ifib.de

[3] http://www.epractice.eu/cases

In several IOP frameworks organizational IOP serves as a container for many different issues, which could not be clearly assigned to the other layers, thus mixing different dimensions and not really providing guidance. It is the objective of this paper to contribute to an improvement of IOP frameworks and the orientation they provide by distinguishing three dimensions of organizational IOP, which are based on operational indicators and allow for an empirical classification and comparative analyses of good practice cases. This paper starts with a review of different IOP frameworks in order to define what has to be made interoperable and then argues that present definitions of the layer of organizational IOP should be confined to technical standards for linking workflows and business processes, while all other organizational aspects should be assigned to two other cross-cutting dimensions which do not only apply to the layer of organizational IOP, but to the other layers as well, and which deal with the “Who” and “How” of achieving interoperability and interoperation, i.e. an actor perspective. We may also speak of three different but complementary views. As it will be explained in more detail in the following sections, we will call them political governance and IT governance of IOP.

For these two cross-cutting organizational dimensions, characteristics and empirical indicators have been derived from the MODINIS IOP Study’s good practice cases and are proposed for an empirically assessed taxonomy, on which future comparative research could build and investigate, which institutional arrangements have been chosen for achieving IOP of different services or for similar services in different countries. At the present stage of research, the selection of indicators and their operationalization is presented in order to receive feedback by the expert community regarding plausibility and usefulness. Therefore comments to this paper are highly welcome and will be considered in the ongoing research heading for a refinement of the classification presented here (e.g. in a Community on the ePractice.eu portal?).

3 Review of selected interoperability frameworks

The European Commission has launched a Communication with particular focus on IOP for pan-European eGovernment services (CEC 2006a). But IOP is also of great importance for the eGovernment development in each Member State. The periodic benchmarking study of eGovernment in Europe explains differences of progress between Member States to a large extent by differences in achieving IOP between different government levels (CEC 2006b, 2007).

The European Interoperability Framework for Pan-European E-Government Services (EIF) developed within the EU program IDABC (Interoperable Delivery of European E-Government Services to Public Administrations, Business and Citizens) (IDABC 2004) has established itself as a reference model for several national IOP programs of Member States. At present it is under review and a new version has been drafted for discussion in July 2008 (European Communities 2008). Similar to the EIF, there are IOP initiatives, frameworks or programs within the eGovernment plans of most Member States. They are summarized in the MODINIS IOP Study mentioned above (Tambouris et al. 2007). Several international bodies have developed interoperability frameworks as well (see Peristeras & Tarabanis 2006).

An IOP framework shall fulfil several purposes. It shall list measures or options that are suitable and necessary to create IOP among separated information systems. In a pragmatic aspect, it shall support the practical planning of systems for several administrations by listing the topics that have to be coordinated and the suitable standards and methods. Thus a communication basis for the developers is created. At the same time, it allows the allocation of tasks. In other words, it gives structure to a complex field, provides common terminology where similar things are termed differently and suggests a classification in order to recognize similarities and differences. This is mainly achieved by assigning different standards for data exchange to three or four different layers of IOP:

- The European Interoperability Framework (EIF) differentiates the three layers of technical, semantic and organizational IOP. The draft of the second version adds the layers of legal IOP and the political context (European Communities 2008).
- In a similar architectural model, the European Public Administration Network (EPAN) adds the layer of structured customer contact and support and, besides the four layers, introduces the aspect of governance as a cross-cutting issue (EPAN 2004).
- In a white paper with the title "Standards for Business", the European Standardization Institute ETSI introduces the layer of syntactic IOP between the technical and the semantic IOP (ETSI 2006).

While the MODINIS IOP Study adopts the three layer classification of the EIF, we propose to pick up the ETSI distinction between a technical and a syntactic layer because regarding to institutional settings there are significant differences between the two.

Considering the purposes of IOP frameworks to provide guidance for achieving IOP, the classification of different layers is necessary, but by far not sufficient step, because it only refers to "What" has to be made interoperable by which technical means, but not "How" these standards are established and implemented and "by Whom"; i.e. the actor or governance perspective is missing. And even regarding the "What" present knowledge about standards on the four layers is quite different (cf. Table 1).

Table 1. Four Levels of Interoperability

Layer of IOP	Aim	Objects	Solutions	State of Knowledge
Technical IOP	Technically secure data transfer	Signals	Protocols of data transfer	Fully developed
Syntactic IOP	Processing of received data	Data	Standardized data exchange formats, e.g. XML	Fully developed
Semantic IOP	Processing and interpretation of received data	Information	Common directories, data keys, ontologies	Theoretically developed, but practical implementation problems
Organizational IOP	Automatic linkage of processes among different systems	Processes (workflow)	Architectural models, standardized process elements (e.g. SOA with WSDL, BPML)	Conceptual clarity still lacking, vague concepts with large scope of interpretation

While technical and syntactic IOP deal with established standards such as TCP/IP and EDIFACT or XML developed and issued by international standards organizations, for semantic IOP there are concepts and methods available, but which are not yet standardized, and for organizational IOP it is by far less obvious what has to be standardized, who could develop and establish appropriate standards, and what is necessary for their operation and maintenance. Some requirements for organizational IOP, in particular in B2G and G2G relations, are defined in the ICT Industry Recommendations to the EIF (Computing Technology Industry Association 2004).

The following box quotes the definitions of organizational IOP in selected frameworks. Compared to the layers of technical and semantic IOP, for organizational IOP

– the definitions are much more heterogeneous,

– the assigned issues are much more vague,

– there are almost no classifications of options available for solving these issues.

One can get the impression that the layer of organizational IOP is filled with all those issues, which turns out to be necessary after IOP has been achieved on the other layers below.

Definition of organizational IOP in different framework concepts

IDABC EIF v.1.0

Organizational interoperability is concerned with "defining business processes and bringing about the collaboration of administrations that wish to exchange information and may have different internal structures as well as aspects related to requirements of the user community" (p. 16).

IDABC EIF draft of v.2.0

Organisational interoperability concerns a broad set of elements of interaction, including business processes, business interfaces such as email, web portals, etc., business events within and between administrations, and "life" events, involving the external parties: businesses and citizens. This aspect of interoperability is concerned with how different organisations such as different Member State Administrations collaborate to achieve their mutually beneficial, mutually agreed eGovernment service-related goals. The partners need to reach detailed agreements on how their processes will interact (synchronize and cooperate) in order to deliver “public services where needed”.

Organisational Interoperability in practice means the seamless integration of business processes and the exchange of information that they manage between the organisations. (from EIF v1).

Organisational Interoperability aims at addressing the requirements of the user community by making services available, easily identifiable, accessible and user-oriented. Organisational interoperability occurs when actors agree on the why and the when of exchanging information, on common rules to ensure it occurs safely, with minimal overhead, on an ongoing basis, and then draw up plans to do all these things, and carry them out.

EPAN

Organizational interoperability "is concerned with the coordination and alignment of business processes and information architectures that span both intra- and interorganisational boundaries. Coordination of business processes across organisational boundaries is essential if a single, aggregated view of a service from the customers' perspective is to be achieved. It is suggested that administrations could develop an exemplar scheme that would define standard approaches to each of the main requirements of any public service and use this exemplar to benchmark all other services; that common functionality could be provided on a shared basis through a broker service to reduce development, deployment and operational costs to the public administration and to each service fulfilment agency, and to ensure consistency of experience for users of services across all agencies in the public sector through the use of agreed standards across all services; that expenditure reviews could be undertaken to ensure that financial priority is given to those schemes that comply with the structured customer support services set out above and with interoperability standards; and that each administration could develop a central programme of organisation development assistance and funding to bring this change about" p. 5/6.

ETSI

"Organisation interoperability, as the name implies, is the ability of organisations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems overwidely different infrastructures, possibly across different geographic regions and cultures. Organisational interoperability depends on successful technical, syntactical and semantic interoperability" (p. 6).

The definitions of organizational IOP mix methods and standards for the technical linkage of business processes (process organization) with questions of the organization of support functions, which cannot be assigned to one layer only, but which apply to all layers. With the more differentiated definition of organizational IOP in the draft of the new EIF v. 2.0 this break of systematization has not changed, but rather even increased by adding the layers of legal IOP and political context on top - which obviously touches issues on all other layers.

4 Distinguishing three organizational views

As mentioned, the EPAN framework provides greater conceptual clarity by separating the dimension of governance and considering this aspect as a cross-cutting issue concerning all layers (EPAN 2004). Also, the ICT Industry Recommendations to the EIF (Computer Technology Industry Association 2004) differentiate between those aspects that are based on legislation, regulations and court findings on the one side and the technical and functional aspects of IOP on the other.

In other words, different but complementary views are introduced referring to "What” is standardized on one side and “Who” develops and establishes these standards, as well as “How” operation and maintenance of IOP standards is organized on the other side. This “Who” and “How”-perspective, called “governance” in the EPAN framework, however still covers different aspects which need further differentiation.

The EPAN framework defines Governance of Interoperability as being “concerned with the ownership, definition, development, maintenance, monitoring and promotion of standards, protocols, policies and technologies that make up the various elements of an interoperability architecture” (EPAN 2004, p. 11). It emphasis the need for coordination of all government agencies within a Member State in order to overcome insular views, to reduce cost and to enable new and innovative ways of working across organizational boundaries. The framework, heavily influenced by the Irish IOP Framework, suggests that ideally the technical and semantic IOP standards should be governed under the authority of one single agency in a Member State while the responsibility for the different issues of organizational IOP, according to the government structure in a Member State might be assigned to different agencies. This is a very particular proposal which is not feasible in all Member States and does not cover the whole range of governance forms usually subsumed under this heading (e.g. hierarchies, markets and networks), while at the same time mixing the political issue of institutional settings, where standards are developed and how they are established or enacted, with issues of implementing these standards by providing certain IT-services. We therefore suggest to separate these two views. The institutional aspect neatly fits to the established understanding of governance. But there is also a debate under the heading of IT-governance dealing with issues of management of IT-infrastructure and services. We propose to capture both subjects by distinguishing between political governance and IT-governance or an institutional and an IT-service view.

"What" has to be standardized: The functional view

In line with the definitions of technical, syntactic and semantic IOP which are confined to technical and functional standards, this aspect of what so far is called organizational IOP should also be restricted to technical and functional standards for the multilateral alignment of business processes across organizational boundaries, i.e. standards for process modelling, architectures or choreographies. By building upon or including technical, syntactic and semantic standards they finally allow the seamless networking between different ICT systems. A prominent example are Service-Oriented Architectures which, by using standardized business process definition languages allow the common description of interorganizational processes, e.g. web services defined in WSDL (Web Services Definition Language) or BPML (Business Process Modelling Language). In order to avoid misunderstandings because of the multiple use of the attribute "organizational" we suggest to name this layer "Business Process IOP".

Political Governance: The Institutional View

Standards for IOP are established in different organizational setting and by different institutional means. There is not one common governance structure for all layers of IOP. Protocols at the technical layer are mostly defined by national and international standardization committees, including Internet working groups, while data formats, ontologies and so forth for creating semantic IOP are - due to their more concrete relation to a particular context - mostly developed by industrial or sectoral organizations (industrial associations, professional bodies, local government associations, etc.). They are either negotiated by the administrations directly concerned or by superior administrative agencies, or established by ordinance or legislation.

IT-Governance: The IT-Service View

Once standards are developed and their implementation has been decided, a lot of questions remain of how to organize and manage for the effective operation and maintenance of the data exchange. When analyzing ordering and billing between industry and retailing we found that ordering and billing information between retailing and producers of brand articles is not exchanged directly, but via Value Added Networks with intermediaries providing certain services such as conversion of data formats, providing up-to-date directories, authentication or authorization services and many more. They can be called clearing houses, generalizing from the inter-bank clearing (Kubicek 1993). For some time standards have been developed to assess IT-services: ITIL (Information Technology Infrastructure Library) and CObIT (Control Objectives for Information and related Technologies) provide criteria for assessing the quality and maturity of the IT-service management. IT-service management in turn is conceived as one field of IT-governance (for an up to date discussion of IT-governance in relation to e-government see the contributions to the IT-governance Community on the ePractice portal[4].

To summarize this discussion, we suggest distinguishing three organizational dimensions or views of IOP. They highlight different kinds of measures that have to be taken whenever IOP has to be achieved for an eGovernment service provided by two or more agencies.

[4] http://www.epractice.eu/community

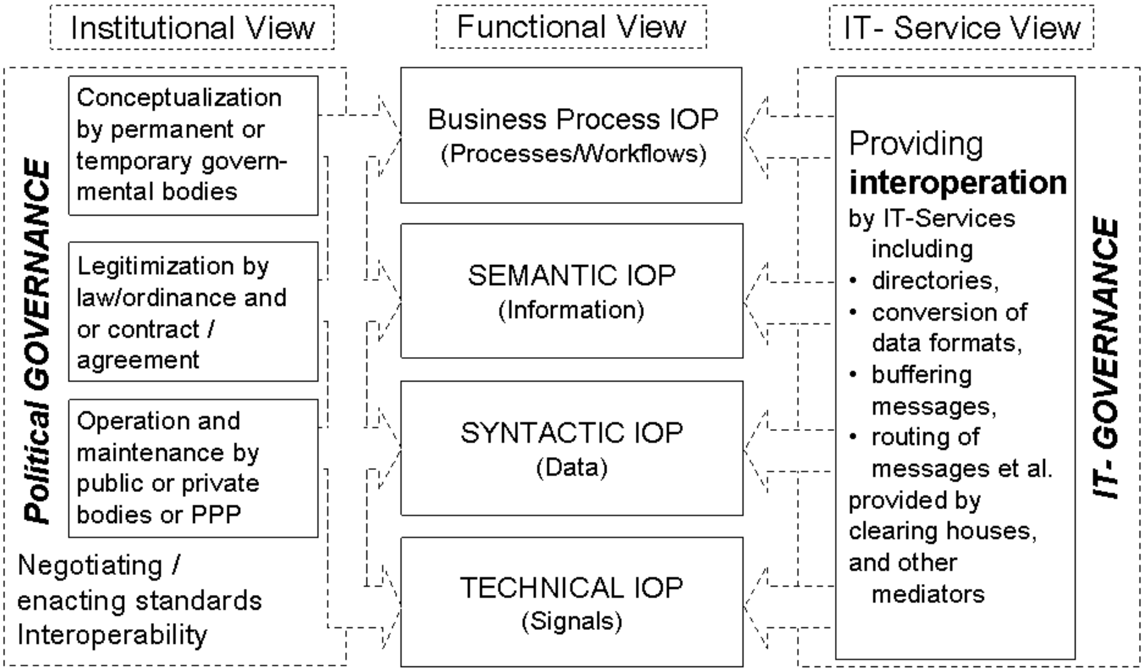

Institutional View
Functional View
IT- Service View
Political GOVERNANCE
Conceptualization by permanent or temporary govern-mental bodies
Legitimization by law/ordinance and or contract / agreement
Operation and maintenance by public or private bodies or PPP
Negotiating / enacting standards Interoperability
Business Process IOP (Processes/Workflows)
SEMANTIC IOP (Information)
SYNTACTIC IOP (Data)
TECHNICAL IOP (Signals)
Providing interoperation by IT-Services including
• directories,
• conversion of data formats,
• buffering messages,
• routing of messages et al.
provided by clearing houses, and other mediators
IT- GOVERNANCE

Figure 1. Layers of Interoperability, their Governance and Provision

In the next two paragraphs we will propose sub-dimensions and empirical indicators, derived from the MOIDINIS IOP Study's good practice case collection in order to differentiate relevant aspects and available options.

4.1 The Political Governance of Interoperability

As mentioned, the EPAN framework introduces the governance of IOP as a separate cross-cutting issue, but in a very special way, and does not cover the whole range of different government forms. The MODINIS IOP Study mentions the three basic forms of governance: market, hierarchy and networks, but does not illustrate how these may be applied in the particular context of governance of IOP for eGovernment services. Looking at the IOP discussion and literature in general there is no classification available on the different arenas where particular semantic and organizational interoperability have been negotiated and decided. Some hints can be found in the TERREGOV organizational case studies (Bousson & Keravel 2005). There is some research on intergovernmental cooperation for achieving interoperability (see Scholl & Klischewski 2007 for an overview) which is mostly case-based, with a strong focus of integrating information systems and does not provide a classification of the different forms of governance for achieving semantic and organizational interoperability. Therefore our research project adopts an inductive approach, looking for patterns in the collection of good practice cases.

When looking for market, hierarchy or network-like patterns in the 32 detailed case descriptions in the MODINIS IOP Study we found that there was not only one governance structure in each case. The planning and decision-making authority rather shifted in the course of three different phases of the development process.

In a conceptualization phase we found working groups and ad hoc committees as well as staff units, mainly composed of experts from the respective application contexts and ICT specialists. The organizational forms in this phase can be distinguished by the degree of institutionalization and representation. Sometimes the IOP standards at the organizational and semantic level are elaborated in existing permanent institutions, sometimes by ad hoc groups put together for a particular IOP project. Representation refers to the extent to which the different sectors or levels of government, which will be affected by a standard, are represented in the respective working group, including providers, suppliers and operators. There could be either no representation of such concerned agencies, the representation of selected pilot or of all concerned agencies.

Table 2. Degree of Institutionalization

	Existing institution	New institution
Permanent	e.g. national Ministries in the e-enabled child benefit service in Ireland	e.g. Crossroads Bank for Social Security in Belgium
Temporary (ad hoc group)	e.g. the working group EDIAKT II in the standardized e-form exchange project in Austria	e.g. the OIO Data Standardization Committee in OIO-XML project in Denmark

Table 3. Degree of Representation

Representation degree	No participation of users	Participation of selected pilot users	All user groups represented

Standards elaborated by such working groups are in most cases proposals, which have to be adopted, issued, recommended or made mandatory by authorized bodies. They need legitimization by law or ordinance, contract or agreement or just by the decision of an authorized and recognized board. In contrast to e-business, in the 32 European cases, almost all semantic and organizational IOP standards for nationwide services have been established by law or ordinance, while on the regional level contracts or agreements were most frequent.

Table 4. Legitimacy and Authorization of Standards

	Mandatory (Obligation)	Voluntary (Recommendation)
Law, Ordinance	e.g. use of the X-Meld standard in Civil Registration in Germany	e.g. integration with the CBSS for social security benefits in Belgium
Agreement, Contract	e.g. use of RTA2 forms in the Road Traffic Accident project in UK	e.g. OIO-XML standards in Denmark

In a third phase, standards, which have been recommended or made mandatory, still have to be implemented and put into operation by assigning certain tasks to certain organizations or units. They can be public or private or public-private partnerships. In many cases tasks of control or supervision are assigned to boards or committees, in particular for promotion, diffusion, maintenance and updates of the respective standards, while tasks of operation are assigned to governmental agencies, joint ventures or private enterprises as service providers.

Table 5. Organization of Maintenance and Operation of Standards

	Public	Private	PPP
Maintenance	e.g. KoopA ADV for the X-Meld standard in Germany	e.g. the Danish Bibliographic Centre in Bibliotek.dk project	e.g. e-invoice consortium in Finland
Operation	e.g. KoopA ADV for the X-Meld standard in Germany	e.g. e-invoice service providers in Finland	e.g. eID card service providers in Estonia

4.2 IT Governance for Interoperation

Once standards have been enacted they have to be implemented and put into operation. This is usually done by defining certain IT-services which support the primary eGovernment services, such as directory or format conversion services, and by looking for appropriate service providers within government or on the IT-service market. In this respect the same coordination problem arises as for the primary eGovernment services mentioned at the beginning of this paper. Decisions have to be taken about the most effective and efficient degree of centralization and standardization. So far there is no classification or listing of what might be centralized and standardized in order to provide interoperation, respectively which kind of services should be provided for achieving this purpose.

Again by adapting an inductive approach we looked at the MODINIS IOP Study's good practice cases for what is standardized and what is centralized in interorganizational data exchange networks and we identified the following provisions for interoperation:

1. standardized directories (same directory is available in each involved unit) providing the address data for routing,
2. standardized data exchange formats on the syntactic layer,
3. standardized data keys or ontologies on the semantic layer,
4. common workflow definitions to describe the source and target processes of the exchange.

In order to support the application of these standards, we find intermediary units, which serve as central service providers for

1. the routing of messages via a central directory,
2. the conversion of data exchange formats,
3. providing access to files of selected (master) data,
4. maintenance of directory data,
5. workflow control (e.g. process control, validation, quality control, tracking and tracing).

It is obvious that in all cases, where messages are exchanged between different organizations, some kind of routing is necessary based on directories to find and determine the target address. Instead of each participating organization individually maintaining such a directory, it is much more efficient to have one central provider who maintains and updates this directory. In order to exchange data between automated processes, there is also a need to define the source and target workflow as well as data exchange formats. Examples are applications for social benefits, notice of change of address or invoices. In some cases, standardization covers the syntax of the messages, e.g. XML schemes for an order; in other cases the meaning of certain data fields is standardized as well, e.g. a unique citizen or business number in an application form or a unique article number in an order or invoice. Again, a central unit may maintain a database with this kind of reference data more effectively. And if there are several formats, it may provide a conversion service as well. So the different elements are not necessarily alternatives but may build on each other.

To adopt the view of IT-governance and IT-service management leads to considering an additional sub-dimension dealing with the maturity level of IT-service management which deals with the precision of service definitions, support and service levels among others.

5 Reflecting the usefulness of the operationalization

At this moment the cases are analyzed and assigned to the operationalized subdimensions of IOP. Thus a descriptive empirical distribution can be generated. Criteria for the quality of such a taxonomy are the exclusiveness of the values attributed and the reliability of the assignment, i.e. whether different reviewers assign the same attributes to a particular case.

From a pragmatic point of view, there is the question whether the presented three dimensions of organizational IOP reflect reality and whether the classifications and kinds of measures on each of the dimensions cover the relevant items. These items shall allow the support of the decisions that had to be taken by public authorities in order to provide for and guarantee interoperation and interoperability. Are there other measures, which should be considered? Are they still too general and should be further differentiated?

From a scientific or analytical point of view, there is the question whether this classification allows to identify certain patterns and relations. One question regarding this aspect is whether there is an order of the various kinds of actions on each of the two sub-dimensions of interoperation (centralization and standardization). Do they have a cumulative structure, i.e. is there a rank order according to which a measure ranked higher only appears where all the measures ranked lower exist as well?

The analysis of these relationships between different measures and the search for patterns, as well as the examination of the different governance aspects, is subject of an ongoing research process which started in May 2008. We would like to discuss the concept of the three organizational dimensions of interoperability and the suggested operationalization with the expert community, either to receive support for building the analysis of these propositions or to get suggestions for changes in order to better meet the information needs of those working on IOP and to whom the interoperability frameworks should provide guidance and support.

Concerning the recently published draft of the EIF 2.0, we suggest rethinking the basic structure with the organizational and legal IOP on top of the technical and semantic IOP and to adopt the distinction between the cumulative layer structure and the cross cutting dimensions of political governance and provision of interoperation (IT-governance).

References

Archmann, S., and I. Kudlacek (2008): Interoperability and the exchange of good practice cases. In: European Journal of ePractice, No 2: New e-ways of doing the Government's job, February 2008. Available at http://www.epracticejournal.eu/issues.

Bousson, A. and A. Keravel, Political (2005): Organizational and Economic Effects in Networked Public Organizations: Organizational Case Studies. TERREGOV Project IST 507749. Deliverable D 6.8, 31.12.2005. Available at http://www.egovinterop.net.

CEC (2006a), European Commission, Communication from the Commission to the Council and the European Parliament COM 45 – Interoperability for Pan-European eGovernment Services. Available at: http://europa.eu.int/idabc/servlets/Doc?id=24117.

CEC (2006b), European Commission, Directorate General for Information Society and Media: Online Availability of Public Services: How Is Europe Progressing? Web-Based Survey on Electronic Public Services. Report of the 6th Measurement. June 2006. Available at: http://ec.europa.eu/idabc/servlets/Doc?id=25150.

CEC (2007), European Commission, Directorate General for Information Society and Media: Online Availability of Public Services: The User Challenge Benchmarking. The Supply Of Online Public Services. Report of the 7th Measurement. September 2007. Available at http://www.epractice.eu/document/3929.

Computing Technology Industry Association, Inc. (2004): European Interoperability Framework – ICT Industry Recommendations. White Paper. Brussels, 18. February 2004. Available at: http://www.comptia.org/issues/docs/interopwhitepaper0204.pdf.

EPAN (2004), European Public Administration Network, eGovernment Working Group: Key Principles of an Interoperability Architecture. Brussels. Available at http://www.epractice.eu/document/2963.

ETSI (2006) European Telecommunications Standards Institute: Achieving Technical Interoperability – the ETSI Approach. ETSI White Paper No. 3. By Hans van der Veer (Lucent Technologies) and Anthony Wiles (ETSI), October 2006.

European Communities (2008), Draft document as basis for EIF 2.0. Available at http://ec.europa.eu/idabc/en/document/7728

IDABC (2004): European Interoperability Framework for Pan-European e-Government Services (EIF) Version 1.0. European Communities, Luxemburg.

Kieser, A. and H. Kubicek (1993), Organisation. 3rd edition, Berlin, New York, De Gruyter.

Kubicek, H., Millard, J. and H. Westholm (2007), Back-Office Integration for Online Services between Organizations, in Anttiroiko, A.-V. and M. Malkia (eds.), Encyclopedia of Digital Government. Vol. I, Hershey IDEA Group, pp. 123 - 130.

Kubicek, H. (1993): The Organizational Gap in Interbranch EDI Systems, EDI Europe, Vol. 33. No. 2, pp. 105 – 124.

Kubicek, H., and R. Cimander (2005): Interoperability in eGovernment – A Survey on Information Needs of Different EU Stakeholders, European Review of Political Technologies (ERPT), Vol. 3, pp. 59-74.

March, J. G. and H. A. Simon (1958): Organizations, John Wiley.

Millard, J., Iversen, J. S., Kubicek, H., Westholm, H. and R. Cimander (2004): Reorganization of Government Back-Offices for Better Electronic Public Services – European Good Practices (Back-Office Reorganization). Final Report to the European Commission, Institute for Information Management Bremen GmbH and Danish Technological Institute. Available at http://www.epractice.eu/document/3187.

Peristeras, V., and K. Tarabanis (2006): The Connection, Communication, Consolidation, Collaboration Interoperability Framework (C4IF) for Information Systems Interoperability, International Journal of Interoperability in Business Information Systems (IBIS), Vol. 1, No. 1, pp. 61-72.

Scholl, H. J., and R. Klischewski (2007): E-Government Integration and Interoperability: Framing the Research Agenda. International Journal of Public Administration, (IJPA), Vol. 30, No. 8-9, pp. 889 – 920.

Tambouris E., Tarabanis, K., Peristeras, V. and N. Liotas (2007): Study on Interoperability at Local and Regional Level. Prepared for the eGovernment Unit, DG Information Society and Media, European Commission, Feb. 2007. Available at: http://www.epractice.eu/document/3652.

Authors

Herbert Kubicek
Professor of Applied Computer Science, University of Bremen
Executive Director, Institute for Informationmanagement Bremen (ifib)
kubicek@ifib.de
http://www.epractice.eu/people/kubicek

Ralf Cimander
Researcher
Institute for Information Management Bremen (ifib) / University of Bremen
cimander@ifib.de
http://www.epractice.eu/people/cimander

European Journal of ePractice · A publication of epractice.eu

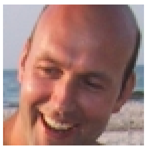
Case Study: Interoperability in the EU Services Directive implementation

According to the European Services Directive, all member states have to support a genuine market in services by simplifying the communication between competent authorities and businesses by 2010. A so called Point of Single Contact (PSC) is supposed to assist in the complete life cycle of a business. At the same time, service providers should be able to do all their interactions electronically.

The directive is an interesting move to push the member states towards a more cooperative and process-oriented electronic government. However, along with this directive, the governmental institutions at all levels - from local authorities to federal governments - have to cooperate, at least to interact with each other. Therefore one of the major preconditions to meet the overall objectives of the directive is to achieve interoperability between the competent authorities, and between PSCs and authorities.

The Fraunhofer Institute for open communication systems (FOKUS) has been working since 10/2007 on an architectural framework and has built various prototypes to show possible technical configurations to meet the requirements of the EU Services Directive in Germany. The prototypes are not complete production-ready implementations by themselves, but they are useful to discuss further details and to-do’s. Current work continues with the incorporation of identity frameworks such as the federID-Open Source Project or the Identity-Metasystem.

With these results in mind, we realize that most of all there is a need for the standardization of Identity and Access Management (IAM) on the political, organizational and semantic levels. Technical interoperability between the EU-SD stakeholders is compulsory, not a feature. An appropriate means to achieve that interoperability and to discuss building blocks in an overall architecture is to create reference implementations based on open source software.



Christian Breitenstrom

Jens Fromm

Fraunhofer FOKUS

Keywords

EU Services Directive, interoperability, identity, federID, prototype, metasystem, simplification, point of single contact, PSC, EU-SD, standardization, identity management

> “ The usage of open source building blocks is an appropriate means to create the vendor neutral prototypes that may be improved by commercial alternatives. “

1 Introduction

1.1 Legal foundation and its key aspects

The EU Services Directive (EU-SD) (Directive 2006/123/EG, see [1], [2]), which was finally approved after three years of discussions in December 2006, will simplify the access to the services market in all member states of the European Union. It aims to minimize existing bureaucratic barriers for service providers (SPs), thus promoting cross-border services within Europe.

As the EU-SD is adopted in 12/2006 there is a timeframe of another 3 years to establish the legal foundation, achieve the organizational reorganization and create the technical infrastructure to implement the directive. As we see it now, the available timespan is used with varying intensity by organizational structures and some of them just start to worry about it.

The first major point is to create institutions that act as Points of Single Contact (PSC) (Article 6) for service providers in all member states. These PSCs have to support the service providers in all administrative processes during the entire life cycle, from the cradle to the grave: from the start up of service activities, during their course and right through to liquidation. The SP has to be provided with means to manage these steps electronically and from distance.

The second point is that all these administrative processes must be available electronically and directly (Article 8) with the competent authority, as well if the service provider wishes to manage them on its own.

The third is that the EU-SD prohibits to hide the internals of service provisioning behind some kind of obscure “PSC-façade”. The process has to be published in a well documented, understandable manner, including price and due information and status requests. The answers to the status requests obviously have to correspond to the published process description.

These three topics create the need to profound interoperation between local, regional and federal authorities, as well as with external support institutions. The processes have to be clarified, documented, streamlined and adjusted, meaning a major challenge for the authorities.

1.2 Basic scenario

As the EU-SD is primarily focused on cross-border activities we see a strong impact of its regulations to the local company in the member state itself. If somebody plans to open up a company in a foreign country, the ability to manage all communications with the responsible authorities electronically is just one aspect among many. Therefore, the majority of communications inbound to the authorities will result from companies within the member state, even after the EU-SD started with complete success.

Most approaches start tying cases together to scenarios that are within the EU-SD scope. Based on a scenario description we can detail the requirements and explain the implications of the EU-SD framework. The incorporation of administrative authorities within these scenarios depends heavily on the chosen domain and circumstances. We began with a very basic scenario incorporating three stakeholders:

- Mr. Pierre Legrand, as a French service provider who wants to open up a bakery shop in Bad Honnef-Germany,
- Mr. Fast, as an employee of the PSC who is responsible for Mr. Legrand’s process,
- Mrs. Weiss, working in the trade office. She is in the position to consider Mr. Legrand’s application.

The scenario is very straight forward. It demonstrates the simple case where only one administrative department is involved. However, at the same time it contains the essential communication paths. The scenario served as an entry point to demonstrate:

- what kind of tasks an employee of a future PSC has,
- what domain of specific support she needs (knowledge-management, case management, CTI),
- where might be privacy issues,

- where the responsibility of the PSC might start or end,
- how Pierre Legrand might find his responsible PSC,
- various other questions.

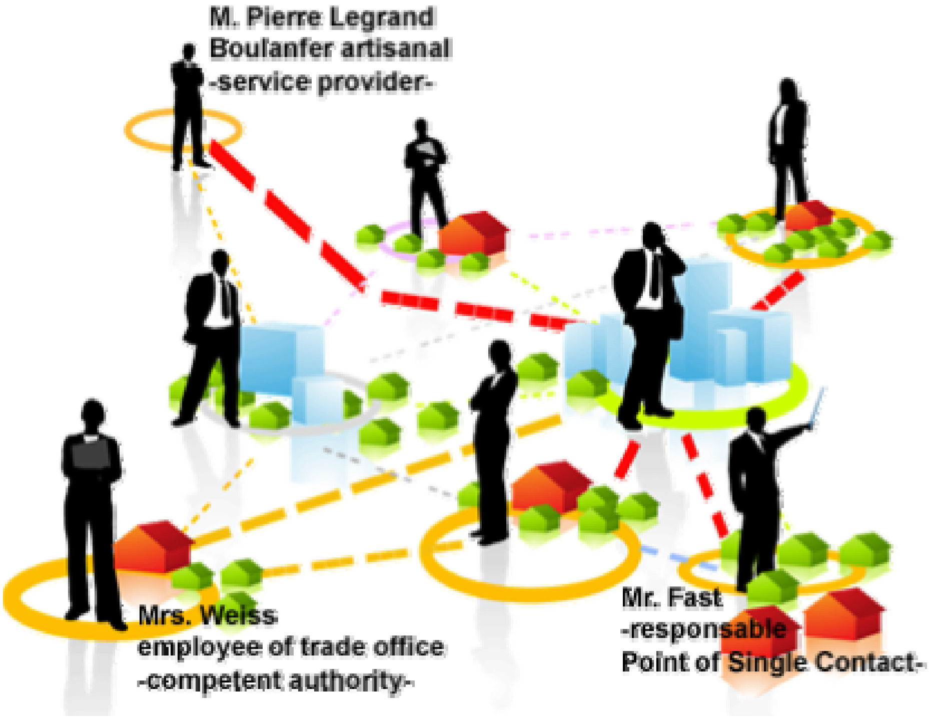
At the end of 2007 Fraunhofer FOKUS built the first prototype with strong support by Microsoft Germany as a potential platform provider for PSCs. The prototype was widely presented and discussed on several occasions like fairs, conferences and workshops.

The resulting discussions lead to a better understanding of necessary domain specific components that make up the infrastructure of a Point of Single Contact. It became very clear that the infrastructures that were planned for the “Call 115 - public administration” project could be used as a base for the EU-SD as well. The scenario made visible that the Point of Single Contact will need a well suited case management and which tasks he/she will have to solve with it. Regarding the knowledge management, it could be shown that former attempts to find the competent authorities based on full-text retrieval mechanisms did not perform sufficiently well and how that problem might be solved using the distributed responsibility directory service. The implementation of a well known process showed that the everyday case of an EU-SD process will require lots of information gathering right at the beginning. A big part of that information was probably gathered in another process and could be reused. This lead to the idea of the online data safe, that could be used by the owner to store his most used data and the electronically signed documents that he receives as a result of the process from the authorities. Seen from that point of view the prototype was a means to collaboratively analyze the requirements of a PSC infrastructure. Instead of looking at it as the perfect solution we discovered the open action items with it.

1.3 Communication paths of a more complex scenario

The scenario easily gets more complex if Pierre Legrand wants not only to sell but also to produce his bakery products in Germany. Then, he needs appropriate permissions from a Health department, has to provide relevant certificates or must meet some other requirements. In the likely case that there are more competent authorities involved, figure 1 shows potential communication paths. Additionally, e.g. in Germany, the responsibilities of the point of single contacts need to be aligned along regional, legal and business related issues.

Figure 1 communication paths in an advanced scenario



The exchanged messages might include notifications of the service provider, status requests, further enquiries by the administration, split payments and communication to external experts. In figure 1 we see that the PSC communicates with several administrations. We know that Pierre might choose to communicate with all of them directly and that the assignment of the PSC to the Competent Authorities is variable over time.

1.4 Interop topics

The above described scenario underlines various challenges, especially in the field of interoperability.

1. Firstly, Pierre Legrand has to find his PSC in one member state. The PSC is relevant according to Pierre's concern (open up a company), to the branch his company belongs to (sell food, produce food, the regulations might vary even between different kinds of bakery products) and according to the region, the city and the location where the bakery should be opened. All of these responsibilities should be maintained in some kind of database (responsibility directory). Because the information in that responsibility directory is to be maintained regionally, we need a standardized way to access and change that information. As we will see, this directory infrastructure needs to contain the catalogue of public sector services, catalogue of geographical entities, competent authorities, responsibilities, processes and others.

2. Pierre wants to use some kind of a user interface to search for "his" PSC, which is presented on its local home portal, that he is accustomed with. So the French portal he uses every day has to get access to the German responsibility directory. We must take into consideration that Pierre needs to be a known person, he must be identified to have access to public services. The identification was done with his local authorities, where he presented his passport, drivers license or comparable. He will not be obligated to repeat this in Bad Honnef again. So the institutions related need some form of trust relationship on the legal, organizational and technical level between each other.

3. When Pierre Legrand "arrives" at the portal site of "his" PSC he needs to read and understand the regulations, responsibilities, proceedings that the PSC works with. So even the website – the presentation layer- has to follow some established user interaction templates to achieve continuous user experience. Interoperability on that layer means continuous user experience. The question was, if we should promote standardization on that field, because the documentation of the process flow (articles 7 and 13) and the answers to status requests are neither trivial nor unimportant. As we see in the general case, Pierre might have contact to several PSCs if he chooses to open up various bakery shops throughout Germany. If the administrative task he orders is essentially the same, then the administrative procedure and the given information about it should be comparable for Pierre.

4. The PSC has to contact several competent authorities and therefore it is economically reasonable to standardize their interface. The interface should be independent from domain, from used domain expert system, from process platform and should even hide whether a service oriented approach is used at all.

5. Access rights have to be established around the directories and around process data. It is obvious that the central information structures are to be secured from unauthorized access, but the access to maintain responsibilities, establish new process versions etc. – the overall governance- has to be easy accessible for a large number of employees because the domain specific know how is decentralized in local administrations. The information in these distributed directories and the process documentation has to correspond to each other and must be historically stored so that long running processes can be handled appropriately. Process data have to be managed with respect to privacy concerns. The connection of formerly separate public services, the need to gather information from Pierre at the beginning of the whole process, bears the risk that this information is used in a way Pierre never wanted. So we created the construct of a data safe, where the user authorises access to. To do that, Pierre needs to know which persons or at least what roles of employees in the administration need access to which data. One might further think on keeping the information in the data safe and to bind it directly to the process, to prevent the data flow in and out of the domain expert system of the administration, but that is a research topic. The simple case, where Pierre only

wants to authorize the administration to work with his data, is already challenging, as the role models for all processes have to be known and maintained in directories (see 1) as well.

As we see, there are plenty of interoperability challenges that must be worked on. So what activities are currently on the way?

1.5 Related Projects in Germany

The Fraunhofer FOKUS activities are embedded in but not paid from the German One Stop Government program (Deutschland Online) initiated by federal and regional government, that got one of the premium projects throughout Germany. The program was started with the intention to develop a “Blaupause” (blueprint) which could be taken as a pattern for the German Bundesländer to implement the EU-SD. The program invited the industry and academic community to submit unpaid contributions, without any guarantee to see the contribution in the blueprint that might create some ROI for the contributing company.

So this might have lead – personal opinion of the author – to the situation that most of the contributions presented by companies contained topics that demonstrate how to implement EU-SD with their own tools and infrastructure. It was mostly not more then to prepare for calls for tender that were expected. The topics in Chapter 1.4 (among many others) were not discussed and other possible pitfalls were not found. It was simply that most of the EU-SD requirements were clear from a bird’s eye perspective but not solid enough to build a home on it. The companies needed some solid regulations to justify their investment to work seriously on it and the political administration alone had not the competence to propose a prototype to see the problems that the companies were asked to solve – a banana problem.

One way out of this could be to order a blueprint that contains the infrastructure and specifications necessary to assure interoperability between different implementations that are based on it. The blueprint might then contain only the “must have” features so that the industry has enough space to improve it and sell their versions. The second point that becomes more and more important is that many small communities cannot afford an expensive platform, so there are more and more affordable solutions on the market that might not survive the next day. These communities could equally use an open source blueprint implementation as a fallback alternative.

2 Proposed architectural framework

The domain specific requirements (part 1), the analyzed component diagrams, their description and interaction between the components (part 2) as well as the technical components and their interfaces (part 3) are documented in the white paper, that is downloadable in English (V.1) and German (V.2) from the FOKUS website. Here are some key aspects of part 3 of this work.

2.1 Implementation goals

Two very basic requirements were imposed:

- The infrastructure needs to discharge the competent authority to a maximum amount from their IT tasks, which are permanently to decide.
- The infrastructure has to provide flexibility in relation to changes of legal and organizational regulations

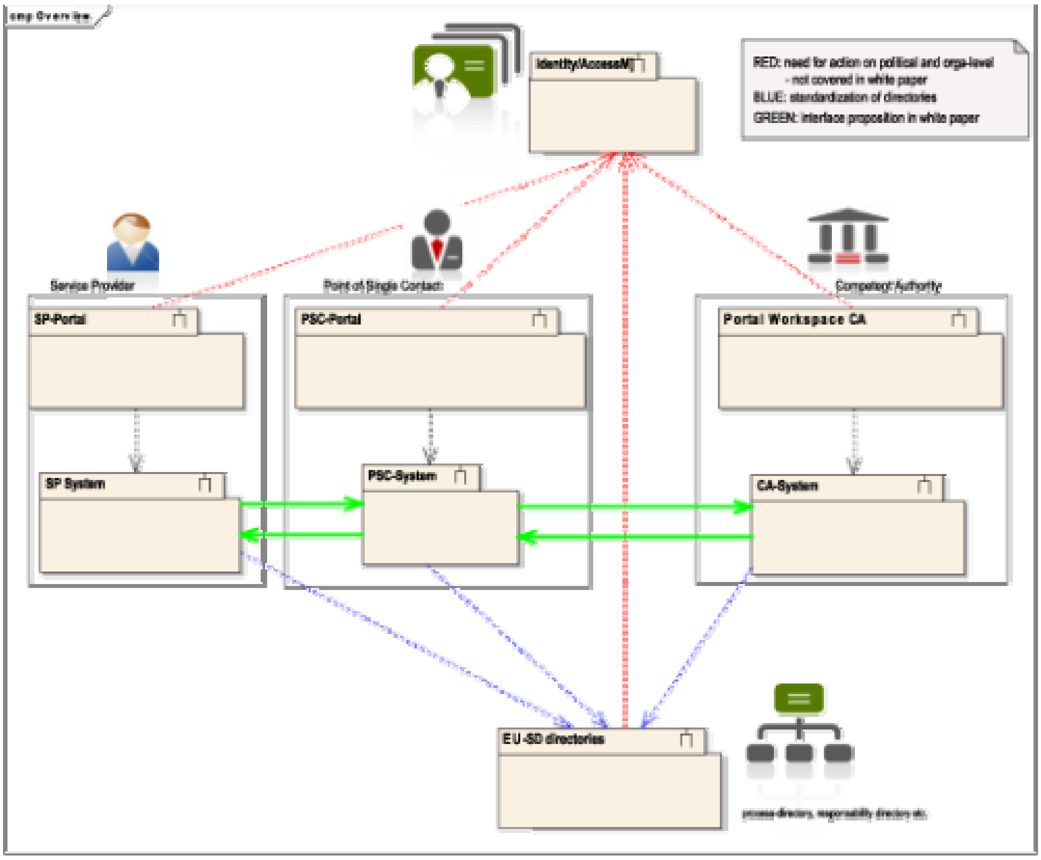
The first point stimulates approaches, where the functionality is offered as a service from competent shared service centres. The management of directory-information and process-descriptions should be well supported and the information should be spread from directories to websites, where it is available for the service providers so that there is only one information source that has to be managed.

The second premise leads to service oriented architectures, as they are today’s IT answer to provide business flexibility and manageability.

2.2 Proposed Interfaces

To solve at least the interoperability-problem between Points of Single Contact and Competent Authorities we proposed the interfaces shown in figure 2.

Figure 2. Necessary work to be done and proposed interface standardization (green)


cmp Overview
Identity/AccessM
RED: need for action on political and orga-level
- not covered in white paper
BLUE: standardization of directories
GREEN: interface proposition in white paper
Service Provider
Point of Single Contact
Competent Authority
SP-Portal
PSC-Portal
Portal Workspace CA
SP System
PSC-System
CA-System
EU -SD directories
process-directory, responsibility directory etc.

On the left hand side the service provider has its portal with an underlying basement that is necessary to receive notifications about the initialized processes on the PSC or CA sites. In the middle there is the portal of the point of single contact that may be used by the service provider, and on the right side we see the competent authorities. As shown in figure 1, the most communication will result between PSC and CAs. So we created web service definitions for an abstract process-interface P for PSCs and CAs that contains the operations:

- ProcessInitialization: initialization of process-type
- ProcessStart: add necessary data to the initialized process,
- ProcessChange: change process state (see chapter 2.3),
- ProcessDataChange: change process data- used whenever a CA has some results or the SP adds some more information to the process,
- ProcessTypes: read, what process-types are supported by PSC/CA,
- ProcessTransfer, to transfer a running process from one PSC to another,
- ProcessStateInfo: get information about a running process.

Further explanation and the wsdls are available [5]. The interface of the service provider only needs to contain the ProcessInfoNotification operation, which is defined in [5] too.

2.3 Complemental process state model

The definition of interfaces and its operations for usage by PSCs and CAs remains useless as long as there is no common understanding about the states a running process might have. The processes need a starting point and an endpoint, in between it is running but may be stopped temporarily. It is especially necessary to define at which point the time to complete the running task is to be counted. If the process execution with the CA needs more information from the service provider, the counter must be stopped until it has provided this information. So we created the state model corresponding to the operations defined in the interface P.

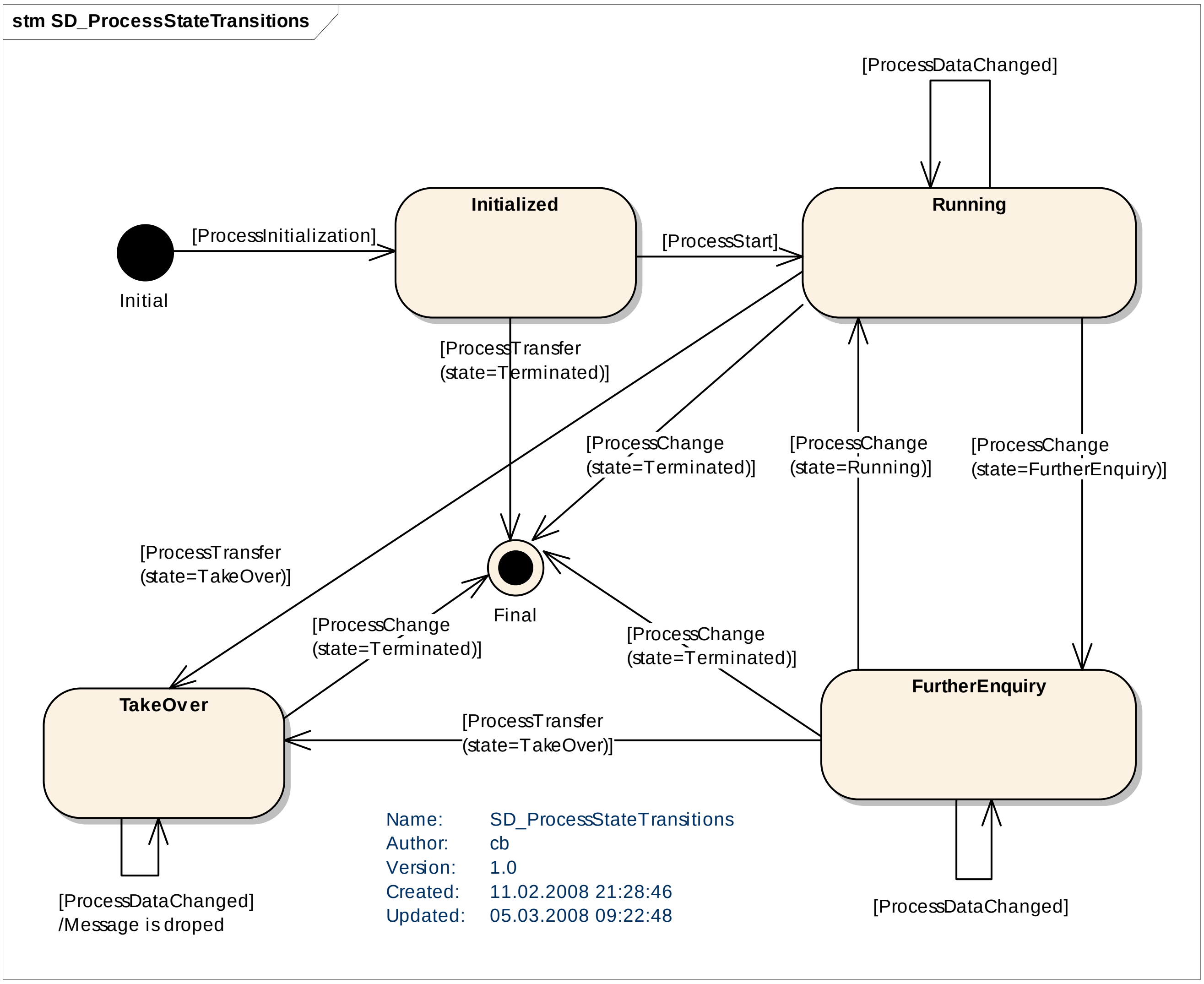

stm SD_ProcessStateTransitions
[ProcessDataChanged]
Initialized
Running
[ProcessInitialization]
[ProcessStart]
Initial
[ProcessTransfer (state=Terminated)]
[ProcessChange (state=Terminated)]
[ProcessChange (state=Running)]
[ProcessChange (state=FurtherEnquiry)]
[ProcessTransfer (state=TakeOver)]
Final
[ProcessChange (state=Terminated)]
[ProcessChange (state=Terminated)]
FurtherEnquiry
TakeOver
[ProcessTransfer (state=TakeOver)]
Name: SD_ProcessStateTransitions
Author: cb
Version: 1.0
Created: 11.02.2008 21:28:46
Updated: 05.03.2008 09:22:48
[ProcessDataChanged] /Message is droped
[ProcessDataChanged]

Figure 3. UML state model corresponding to interface definition

3 Current work

As you saw in figure 2, the red and blue arrows on the picture remain still as work to be done. The blue arrows stand for necessary links between EU-SD infrastructures within authorities and central directories. These central services directories are necessary to find and use the offered administrative services. The red arrows remember the necessary identity management system which connects all the involved parties.

Currently at FOKUS the information model for the directories is defined and some prototype is built to discuss these definitions with an audience from regional and federal administrations.

The bigger topic is to adjust the available Identity Management Solutions so that the different EU-SD sites (PSC portals, CA portals, SP portals) can transfer identity and authorization information in a trustworthy way to each other. We suppose that in an EU-SD context we will have multiple circles of trust, so that we need trust relationships between them. To provide electronic IDs there are currently some EU co-funded projects on the way, e.g. eID/STORK (see [7]) and there exist several well suited regional solutions, e.g. the multi-pki validation authority in Spain (see [8]) or DigiD in the Netherlands (see [9]). On a technical level we have to provide interoperability between different federated identity management (FIM)-solutions (for a closer look into WS-Federation see [10]). We currently test the federID project that consists of well established open source components (see figure 4) in combination with commercially available products to simulate different circles of trust in an EU-SD context.

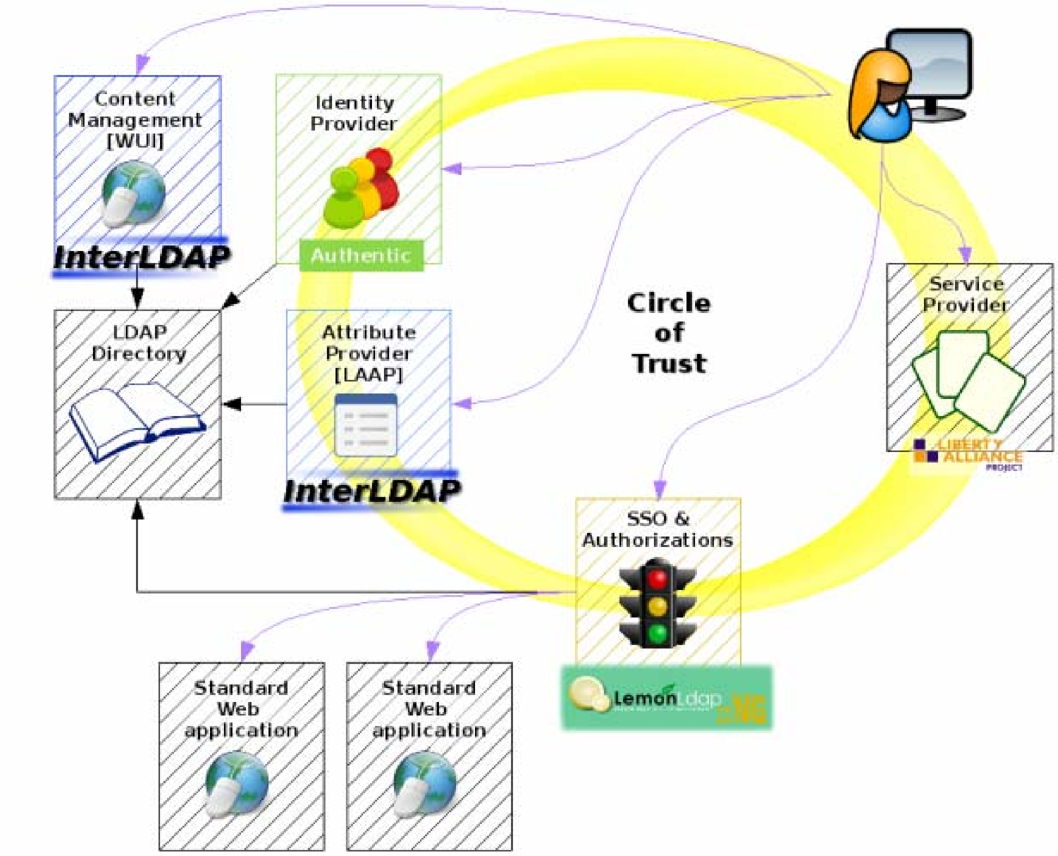


Figure 4. Components of the federID-open source solution, see [6]

Part of that is to address existing privacy concerns with the InfoCard framework. The InfoCard approach overcomes barriers like the storage of user data on external servers by storing private data on the user's side and offering the option that trusted third parties could be responsible for the actual storage of authentication data. The InfoCard itself holds only Meta information on how to actually access private user data from so called "identity providers" (IPs). Identity Providers may be trusted third parties holding a Security Token Service (STS). An improved level of protection is reached before various forms of identity attacks, such as phishing can occur. In particular, the user is in possession of his own data and can decide which information a web site will receive. Different web services can store different data, from different cards. This is possible because InformationCard allows them to have as many digital identities as anyone needs. Fraunhofer FOKUS tests and analyses the various approaches and is building showcases around it (look at eidentitylab.org for further information). To promote the spreading of this approach we built a plug-in for Java-based application servers, called JInformationCard, in order to test InformationCards from various identity selectors such as CardSpace, DigitalMe or Higgins (the plug-in is running on JBoss, Glassfish or WebSphere[1]).

[1] Have a look at: https://www.jinfocard.org

4 Conclusions

As the current development of public administration changes from a task oriented to a more process oriented organization, interoperability becomes the key enabler for modern eGovernment.

The presented white paper became a well known reference in Germany, it influenced the discussion process and some of the current calls for tenders are reflecting requirements that were detailed in the paper.

The founding specifications were achieved using an interdisciplinary effort between people working in administrative boards and the technical staff from Fraunhofer FOKUS. The implementation of prototypes that can be used to discuss the problem space and further detail the requirements play a crucial role.

The usage of open source building blocks is an appropriate means to create the vendor neutral prototypes that may be improved by commercial alternatives. In our show cases we were able to distribute the open source components to third parties that were interested in studying our solution to build their own. Industry partners willing to create open standards are an incredible valuable resource for reviews and should be involved at an early stage of this process.

Acknowledgements

We would like to thank our industry partners BEA Systems belonging now to Oracle Deutschland GmbH, Microsoft Germany GmbH and the team around Clément Oudot that is maintaining the Open Source FederID project.

References

[1] Directive 2006/123/EC of the European Parliament and of the Council on Services in the Internal Market; December 2006

[2] Handbook on implementation of the Service Directive; Luxembourg: Office for Official Publications of the European Communities; 2007

[3] J. von Lucke, C. Breitenstrom, K.-P. Eckert: IT-Umsetzung der EU-Dienstleistungsrichtlinie; Gestaltungsoptionen, Rahmenarchitektur und technischer Lösungsvorschlag - Version 2.0; Fraunhofer IRB Verlag; August 2008; ISBN 978-3-8167-7765-6

[4] Internal Market Information Systems: IMI; retrieved September 29, 2008 from http://ec.europa.eu/idabc/en/document/5378/5637

[5] Fraunhofer FOKUS Website. http://www.fokus.fraunhofer.de/de/elan/publikationen/Infomaterial/white_paper/DLR_2_0/index.html

[6] Documentation on FederID website; retrieved September 29, 2008 from http://federid.objectweb.org/xwiki/bin/view/Main/FederIDComponents

[7] Documentation on eID STORK website; retrieved December 03, 2008 from http://www.eid-stork.eu/

[8] Home page of the Spanish multi-pki validation authority; retrieved December 03, 2008 from http://www.csi.map.es/csi/pg5a12.htm, http://www.epractice.eu/cases/1984

[9] Home page of the Dutch national ID solution; retrieved December 03, 2008 http://www.digid.nl/

[10] Goodner, M., Hondo, M., Nadalin, A., McIntosh, M., Schmidt, D. (2007). Understanding WS-Federation, website; retrieved December 03, 2008 from http://msdn.microsoft.com/en-us/library/bb498017.aspx

[11] Overview on Open Source Identity Systems; retrieved December 03, 2008 http://osis.idcommons.net/wiki/Category:I4_Solutions

[12] Project page PrimeLife, EC funded project to explore privacy and identity management in Europe; retrieved December 03, 2008 http://www.primelife.eu/

Authors

Christian Breitenstrom
IT architect at the Fokus eGovernment Lab
Fraunhofer FOKUS
christian.breitenstrom@fokus.fraunhofer.de
http://www.epractice.eu/people/15195

Jens Fromm
Head Secure eIdentity-Lab
Fraunhofer FOKUS
jens.fromm@fokus.fraunhofer.de
http://www.epractice.eu/people/15310

Interoperability and community building for transformational eGovernment

The latest technological progress has unveiled the enormous capacity for ICT (Information and Communication Technologies) to become a leading force in the modernisation of public administration and has raised the appearance of Transformational eGovernment. The potential for ICT in public affairs is constantly increasing. Considering the countless number of web-based applications – each time increasing in complexity – that have been developed in the last five or six years and are now widespread and popular for private use, one can only think of the possibilities this can offer to public administration and governments.

Many different initiatives and projects are currently being carried out across Europe, aiming towards the promotion of eID and interoperable solutions. Interoperability is, to this date, perhaps one of the most challenging issues for the future of eGovernment in Europe. The development and further implementation of cross-border solutions, which constitute an essential pillar to enhancing the mobility of citizens and businesses in the internal market without encountering electronic barriers, is strictly dependent on interoperability; the best way to ensure its success is through the exchange of experiences and communities of practice.

Sylvia Archmann

Just Castillo Iglesias

European Institute of Public Administration

Keywords

Interoperability, key enablers, eID, eIDM, Transformational eGovernment, communities of practice, COP, identification management, citizen-centric government

> “Governments should put efforts into inclusion, building trust in the new technologies and the promotion of, at least, basic eSkills.“

1 Transformational eGovernment

ICT have impregnated many aspects of our everyday lives, having an impact on our ways of communicating, looking for and sharing information. A myriad of web-based applications have appeared in the last few years, constituting what is known as 'the social internet', providing powerful tools for planning, networking and communicating. The potential of this technology for its use in government or public administration is enormous, both in the day-to-day work of policy making – enabling for instance, more direct contact between politicians or law makers with the centres of expertise – and in the way that public administrations communicate and provide services to citizens. The adaptability of these internet applications, plus its availability across multiple platforms, are an important source of inspiration for similar applications in public services.

The power of eGovernment and ICT to change government and administration has given rise to the concept of Transformational eGovernment. The idea first appeared in the early 2000s in Belgium's eGovernment Strategy, focusing on the use of eGovernment to adapt governmental services to the needs and actions of citizens. Later on, the idea of "Transformational eGovernment" found its place in an initiative by the UK's Cabinet, launched in 2005 under the name "Transformational Government Enabled by Technology" (UK Government, 2005). This initiative also aimed to improve the delivery of services emphasising the use of ICT, thus making them fit for the 21st Century. Transformational eGovernment, thus foresees, in the first place, the delivery of public services through the internet, and the re-design of public services around the citizen, instead of according to the needs of the administration (citizen-centric); secondly, it encompasses the move towards a culture of shared services (standardisation and simplification of procedures fomenting the culture of sharing and collaborating); and thirdly, it aims to strengthen public employees' professionalism and skills, thus leading to a knowledge-powered change within the government's administration.

Besides this, the extension of public service delivery towards ICT seems to be the winning bid for the future of public administration in Europe. Everyday we are seeing more initiatives, pilots, programmes, etc. aimed at developing solid bases on which administrations can cooperate and share information in order to achieve fully functioning cross-border and pan-European[1] solutions. Nevertheless, the preconditions for Transformational eGovernment to become a reality are not only technical (i.e. developing the right software or systems), but also organisational, social and cultural: spreading ICT skills[2] (EIPA, 2005), for instance, has a very important role to play in making Transformational eGovernment a success. Rethinking public administration and modernising it in a way that makes the delivery of public services faster, more reliable, and less burdensome, is, thanks to ICT, something very positive that can increase productivity of the public sector. Yet at the same time, it depends closely on the fact that citizens have access to computers with internet connection and they actually know how to use them. Similarly, citizens have to be assured that the new way of obtaining services from the administration is not only fast, but also secure. Governments should put efforts into inclusion, building trust in the new technologies and the promotion of, at least, basic eSkills.

2 Key enablers: eIDM[3] & interoperability

The i2010 eGovernment Action Plan of 2006, which aimed to accelerate the benefits of eGovernment for citizens and businesses whilst ensuring that eGovernment at national level does not create new barriers for the internal market, established a list of five top priorities to achieve these goals: no citizen is left behind; making efficiency and effectiveness a reality; implementing high-impact key services; putting key enablers in place; and strengthening participation and democratic decision making. Among those, the Action Plan paid special attention to the importance of putting in place the key enablers.

The term key enablers refers to the infrastructure that allows eGovernment services to function properly, for instance, interoperability is considered a generic key enabler. To put it in the words of the European Commission, "Key enablers are the glue that binds eGovernment together" (European Commission, 2007).

[1] 'Pan-European services' refers to cross-border services encompassing the whole of the EU.
[2] Also commonly referred to as eSkills.
[3] Interoperable electronic identification management.

The key enablers foreseen by the Action Plan are eIDM to access public services, the electronic authentication of documents (eSignature) and electronic archiving. These key enablers would allow cross-border projects to have major visibility by putting material tools directly into the hands of citizens. Hence, the Member States agreed to enable by 2010 secure systems for mutual recognition of national electronic identifiers for websites and public administration services. In the case of eID as a way to access public services, interoperability is a crucial pillar; not only at the national level among different authorities or levels of government, but also across Europe in order to move towards cross-border services.

A popular example of what it intends to achieve is that of a retired Belgian citizen spending the summer months on the Spanish coast. Thanks to cross-border interoperable solutions, this person should be able, from the Spanish administration's internet portal and his Belgian eID card, to access his national services – depending on the Belgian authorities (i.e. his pension or social security services) – as well as the services offered by the municipality where he is staying in Spain.

Even though this scenario is not yet completely a reality, several pilot projects are currently being set up involving various European countries testing the interoperability of systems in order to arrive at recommendations for the specifications of a common standard. Despite the hopes put on such projects by the European Commission and the Member States, their great complexity appears to be not only in technical terms, but also in the semantics (systems belonging to different administrations and different Member States should understand the same meaning of the data they are processing) and on the different levels of trust that have a direct impact on the ease by which different instances of government and other relevant stakeholders cooperate.

By promoting interoperability of systems across Europe – and even with more relevance in the case of cross-border interoperability – stakeholders need to take into account that different countries understand different things under the concept of eID, and that the objectives are to help systems to work together, rather than replacing each country's own way of organising itself. Under the concept of eID, for instance, some countries use electronic ID cards, some use passports; for all of them, eSignature is not so closely linked to eID as in others. Therefore, the exchange of experiences between different stakeholders, whether they belong to the public or the private sector, and members of research centres and academia should be encouraged in order to enhance collaboration and better cooperation for interoperability.

There has so far been enormous progress in the promotion of interoperability, both at EU and at the national levels. Following the publication in 2004 of the first version of the EIF (European Interoperability Framework), which is currently under revision, many Member States have developed their own initiatives and other sets of practice guidelines to make their administrative structures fit for collaboration.

The importance of interoperability lies in its potential benefits (Archmann & Kudlacek, 2008). Therefore, identifying the settings when interoperability becomes indispensable is an important step in helping to work towards finding common solutions. The MODINIS Study on Interoperability (EIPA et al., 2007), of which EIPA was one of the authors, identified the following five scenarios in which interoperability is crucial and should, thus be promoted:

- Firstly, between the different services under the same client, namely the grouping of services (for example, according to life events or problematic situations) in order to save resources or to improve the quality of service (one-stop government);
- Secondly, among the different stages of a supply chain that is producing one or more services, for instance, when a single service cannot be produced entirely by a single agency, there is a need for interoperability between data workflow and input from other agencies and offices;
- Thirdly, namely among the agencies in different geographical areas, interoperability refers to the direct transfer of data from the system of one administration to another administration system (mainly geographical);
- Fourthly, among the directory services or documents, namely interoperability between local directories, common metadata about services, as well as algorithms to locate the right agency. One crucial question concerns the common descriptors for services and agencies.

- Finally, in supplementary services (identity management, digital signature, etc.).

Disclosing these five scenarios in which interoperability has such a prominent role was among the most relevant results of the MODINIS study – a fact that is further supported by the number of initiatives, pilot programmes, etc. that have appeared throughout Europe since its publication, and that are focusing on eliminating the shortcomings that make the development of interoperable solutions more difficult.

According to our compromise with the future of eGovernment in Europe, EIPA has been active throughout 2008 in an initiative called "Connecting Public Services Communities" (EIPA & Politech Institute, 2008). This initiative was launched in response to a necessity to establish a community of practice on interoperability to facilitate the networking, dialogue and the exchange of experiences among the most relevant interoperability and eGovernment stakeholders in Europe, and to help establish a trust scenario where the obstacles to overcome can be discussed. With "Connecting Public Services Communities" we acknowledge the importance of sharing experiences among practitioners involved in cross-border services, members of the academia, and other relevant stakeholders as a means for the success of such services. The initiative was launched at the Bled eConference (Slovenia) in June 2008, and continued with a second roundtable in Paris during the World e-Democracy Forum. Furthermore, the most relevant cases and experiences shared during those two meetings have been published in an especially dedicated edition of Politech Institute's European Review of Political Technologies.

During the initiative, efforts on interoperability of different natures have been put on the table: from the development of the Lithuanian National Interoperability Framework following the European Interoperability Framework (European Commission, 2005), to currently ongoing pan-European pilot projects, such as the STORK project (European Commission, 2008b) on interoperable eIDs or the PEPPOL project on eProcurement (European Commission, 2008a). Among the many lessons learned, the cases seen have taught us about the utmost importance of those aspects of interoperability that go beyond technology. A practical totality of the over 20 invited stakeholders have stressed that taking into account the multidimensionality of interoperability (semantic, technical and organisational), is one of the crucial success factors for their projects.

Considering this, as Europe moves towards Transformational eGovernment and it advances towards the creation of more and better interoperable solutions, it is important not to forget that the reason behind all those changes is the will to make life easier for citizens and businesses, as well as to facilitate and enhance their mobility across Europe. Thus, interoperable solutions need to be further developed in Europe, whilst always keeping in mind the concept of Transformational eGovernment. Introducing new services and innovative ways for citizens and businesses to interact with public administration and to get their public services delivered is something truly positive. However, it should never create new burdens or difficulties for them, especially in the short term. Our experience tells us that collaborating and sharing best practices to be able to learn from them is the right way to go. The exchange of experiences and the creation of communities of practice such as "Connecting Public Services Communities" can provide some help towards this.

3 Concluding remarks

This article aims to draw practitioners' attention to the most common trend in European public administration towards eGovernment: moving towards a culture of citizen-centric government, bidding strongly on the use of ICT for the delivery of services, and providing a more helpful and more efficient administration. This is known as Transformational eGovernment and it depends strongly on the success of interoperability in Europe; acting as a generic key enabler for more advanced services to appear, including cross-border services that even aim to reach a pan-European scope. In the article we have seen the utmost importance of those interoperability aspects that go beyond technicalities such as key success factors for advancing in the creation of interoperable solutions and contributing to making cross-border eGovernment services a reality. It is only a matter of time until pan-European interoperable eGovernment will become a reality; we will surely see it in the near future. However, reaching this point involves a long road ahead and plenty of work to do, in which a huge number of actors are involved, as well as an important number of already existing national or local enablers who will have to interoperate with each other. Thus, the key factors for success are the exchange of experiences and promoting common work among the main stakeholders through communities of practice such as "Connecting Public Services Communities".

References

Archmann, S. & Kudlacek, I. (2008). Interoperability and the exchange of good practice cases. European Journal of ePractice, no. 2 Feb. 2008. http://www.epracticejournal.eu/volume/2/document/4338

EIPA (2005). Commissioned by the Luxembourg Presidency of the EU. Study on Organizational Changes, Skills and the Role of Leadership required by eGovernment. Maastricht. http://www.epractice.eu/document/2935

EIPA et al. (2007). Study on Interoperability at Local and Regional Level. Final Version. http://www.epractice.eu/document/3652

EIPA & Politech Institute (2008). Connecting Public Services Communities. European Review of Political Technologies, vol. 7, October 2008. http://www.epractice.eu/document/5184

European Commission (2005). European Interoperability Framework for pan-European eGovernment Services. http://europa.eu.int/idabc/3761

European Commission (2007). Key Enablers. http://ec.europa.eu/information_society/activities/egovernment/policy/key_enablers/index_en.htm

European Commission (2008a). PEPPOL – Pan European Public Procurement on-line. Press release IP/08/785, 23 May 2008.

European Commission (2008b). Stork Project – Secure identity across borders linked. Press release IP/08/824, 30 May 2008.

UK Government (2005). Transformational Government Enabled by Technology. Cabinet Office. London. http://www.cio.gov.uk/transformational_government/strategy/

Authors

Sylvia Archmann
Seconded National Expert
EIPA
http://www.epractice.eu/people/11942

Just Castillo Iglesias
Research Assistant
EIPA
j.castillo@eipa.eu
http://www.epractice.eu/people/13591

Development of a Multi-eID access control system. How to get out of trouble with Open Source

This case study focuses on how the Italian city of Grosseto managed to add highly secure eID-based access control to its ICT existing infrastructure applying a rigorous open source strategy. Developed to solve an interoperability problem, our eID access control system, called Open Portal Guard, has already been used with several foreign eIDs and we have started to seek to replicate our experience in other sites. We believe that the reuse of its open source code by other administrations and private sector service providers may jump-start many into the world of high-security identity management. This is even truer considering that to date a majority of European Member States are either implementing their eIDs strategies or plan to do so in short, and that the software we have developed is freely available from IDABC's OSOR repository.

In addition to promoting the use of our eID access control system, this case study also aims at encouraging the use of the open source approach in general. We hope this article illustrates the high potential for efficiency that comes through working with the community and collaborative development.

Bud P. Bruegger

Municipality of Grosseto, Italy

Keywords
eID, Open Source, Interoperability, Community, collaboration, Osor, security, interoperability, identity, smart card

> “ A simple policy decision to do everything in open source from now on is easy but almost worthless - it has to be brought on the ground, and that is not done by decisions, orders or policy. “

1 The Setting

This case study starts with the city of Grosseto's participation in the second pilot project of the “Carta d'Identita' Elettronica--CIE”, the Italian eID card by the Ministry of the Interior. The tasks assigned to local governments in this project were not only the issuance of eID cards to a large percentage of population, but also to provide on-line services to citizens (and in some cases other administrations).

The city of Grosseto has a significant track record in the field of ICT, having developed some of its key applications (including the population register) in-house since 1977 and acting as an Internet Service Provider to its citizens since 1996. The eID pilot project could thus make use of a solid ICT infrastructure, a variety of pre-existing on-line services, and most importantly, a high level of internal capacity that is surely a key enabler for getting involved in open source. At the beginning of the project, however, the city was lacking any experience with smart cards and strong authentication.

This case study focuses on how the city went about adding highly secure eID-based access control to its existing infrastructure. The system has been in operation for several months now and we have started to seek to replicate our experience in other sites.

The following scenario illustrates the day to day use of our access control system. Citizens, internal staff or authorized personnel of external organizations access some of our sensitive resources that are exposed on the web. To do so, their browser connects to a single point of entry and access control where the browser functionality of identifying oneself based on a user certificate is triggered. No matter which eID card users choose, the access control system verifies the certificate and extracts a single user-ID to present to applications, hiding all differences of the various eIDs. Optionally, pseudonymous user identifiers can be derived for privacy enhancement, roles that users possess can be looked up and a first decision on whether to grant access to the resource is made[1]. The system works with any technology of application server.

2 No Way! Let's Roll Our Own—or how to get yourself in trouble

Life is often spiced up with some real challenges, and it was no different for the eID pilot project. People who care seem to face more challenges than others; and challenges are self-created at times when we explicitly decide to get ourselves in trouble.

Considering that internal development capacity is getting increasingly rare in local authorities, it is not surprising that the pilot project assigned full responsibility for the eID access control system to a technology provider. Our task was to install and use it -and this essay was not supposed to be written-, but life is full of surprises.

Trouble is that we are overly picky people and that we want to continue to promote certain values that we have been able to establish in years of hard work. So there were some characteristics of the offered access control solution that we simply rejected. They included the following:

– The “yearly license tax”: Local government in Italy, like possibly everywhere world-wide, is increasingly faced with small and decreasing budgets. Launching new activities and services is therefore subject to finding specific additional funding, like that provided by our Ministry of the Interior for the eID pilot project. For new services to be sustainable, they can inflict only marginal cost of maintenance, once the funding has ended.

  Our Ministry understands this situation well and has therefore made sure through the contracts that all software developed during the pilot is owned by the ministry and remains at disposal of local governments free of charge also after the pilot[2].

[1] This decision can be further refined in technology-specific settings like an application server (e.g., J2EE declarative access control) or the application itself (e.g., J2EE programmatic access control).

[2] While this approach obviously has a needed and desirable effect of protecting the interests of the public administration, it can also create impediments to a development approach based on open source communities; not being the copy-right holder makes it impossible to decide on the licensing terms, often a prerequisite for collaborative development.

Unfortunately, our technology provider explained to us that this applies to all BUT a small but critical piece of software (a browser plug-in) that predated the pilot project and that they generously made available free of charge during the pilot project. As soon as the project ends, we would then have to pay a yearly licensing fee to be able to distribute this critical piece to our citizens to enable them to use our services.

- Mono-platform: This critical browser plug-in, intended to be installed by all our users, had another shortcoming, namely that it worked only on Windows. We have a policy to provide eGovernment services to citizens no matter their sex, race… or preferred operating system. Our technology provider generously offered to solve the problem by adapting their plug-in to the other platforms at a modest additional cost.
- Proprietary instead of Standard: One of the guiding principles for our ICT infrastructure is the use of standards as much as possible. Proprietary solutions have always gotten us into trouble sooner or later. This is because they are always linked to a certain vendor, are difficult or impossible to combine with products from other vendors and quite often leave you in a crisis at the end of its life cycle or when a vendor fails.

  Almost everyone who needs strong authentication based on certificates (as in our eID) uses the highly stable and ubiquitously implemented standard of Transport Layer Security--TLS (also known as Secure Socket Layer--SSL), which is a well-established work horse on Internet security and is built into all mayor browsers and web servers.

  In contrast, the solution proposed by our technology provider opted to use a proprietary approach instead. While admittedly this choice was well-motivated to adapt to a peculiarity of the eID used in the pilot phase[3], we later learned and demonstrated that it was indeed possible to use a standards-based approach.
- Mono-eID: The proposed system supported a single eID (the CIE of our Ministry) and was specifically designed around the peculiarities of this eID. By law, Italian public administrations, in addition, have to accept the Carta Nazionale dei Servizi (CNS). For pragmatic reasons, we also wanted to support a wide variety of digital signature cards[4] from government accredited private Certification Authorities that are not standardized. Surely, our technology provider would have been happy to extend the system in a separate contract to support the additional cards.
- Technology-specific: The proposed system was implemented in J2EE[5] technology. While J2EE is one of our major platforms, we have many other kinds of technology in operational use and we believe that an authentication and access control system should be technology-neutral.

Enough is enough! Many of us have been married at least once and know that marrying someone is a serious decision and that the prospects are rather bleak when you don't like the bride in the first place. We believe this applies also to technology providers.

3 Swim or sink – well, you asked for it!

Who rejects marriage has to accept life as a single; and this means cooking by yourself, ironing by yourself, and—in some cases—developing your own eID access control solution. It is easier to complain about others than to live up to your own demanding standards. So we had just jumped into cold water without flotation aid and were wondering what it takes to swim. We faced some real challenges:

Resource constraints: Our alternative solution needed to be created with almost zero resources. After all, there was nothing budgeted for this unplanned development.

Acquisition of know-how: Access control and identity management was not part of our core business and we lacked relevant experience. We badly needed to get up to speed as quickly as possible.

[3] Namely that the nationally unique ID was not contained in the authentication certificate—something that has now been "fixed" in the final version of the eID card that is expected to be rolled out nation-wide shortly.

[4] At least those that contain an authentication certificate in addition to the qualified signature one.

[5] Java 2 Enterprise Edition

Sustainability: We needed to find a sustainable solution. It is often easy to develop a first version of a product, but much more demanding to manage its whole life cycle and maintain it over time.

Quality and Security: Governments make very significant investments in achieving a high enrolment of citizens and top of the line security features on eIDs. eIDs are a prerequisite for exposing critical resources and services on-line. An access control system only makes sense if its security-level matches that of the enrolment and eID tokens. This means that the quality of all security-critical components has to be very high—the result of extensive review and testing. It also means that the system has to be designed based on "security thinking", a skill that is not usually part of the professional repertoire of application developers, who focus on features and cut a trade-off between bugs and time to market.

Interoperability—the micro-cosmos of local governments mirrors the macro-cosmos of Europe: Self-similarities across scale, as those found in fractals or in some aspects of nature, are always somewhat awesome and surprising, since we naively expect the very small things to be substantially different from the very large things - the small things to be relatively simple while the large things are complex.

So who would have expected that the eID interoperability problems of a local authority would be highly similar to that of the eID Interoperability planned for Europe by 2010 as decided in the Manchester Ministerial Declaration, part of the i2010 eGovernment Action Plan, and the issues currently addressed by many Member States in the project STORK?

But indeed, our local government problem is composed by very much the same ingredients:

- Multiple eIDs to support: By law, Italian public administrations have to accept both the CIE and the CNS cards in their on-line services. For pragmatic reasons, real-world services cannot rely on every user being in possession of one of these cards and also have to accept a wide variety of non-standardized digital signature cards. This brings the full complexity of managing multiple "Identity Authorities", each of which having a different CA and Trust structure and different ways of identifying the same citizen in the certificates *subject common name*. In one case (that of the pilot-phase CIE card), the certificate even lacks a unique identifier for the citizen.
- Support for credentials that are not certificate-based: While we aim to eventually use eIDs exclusively, we have the need to integrate also pre-existing authentication solutions based on username/password in our authentication infrastructure. This mirrors the European requirement to support all possible authentication credentials including non-certificate credentials such as the Austrian Citizen Card.
- Need for privacy enhancement: In some cases, like in social applications, we provide services that are highly privacy-sensitive. For this purpose, in a nationally funded project ("iDEM") we had to study and implement privacy-enhancement strategies in our access control system to provide "pseudonymity" to our users.

This illustrates how the interoperability problems of local authorities are really highly similar to those in Europe - what changes is mostly the perspective. Local governments have to be highly pragmatic and rapidly find simple and cost-effective solutions. They focus on technical problems, giving much less emphasis on legal and political problems; they have to encompass all credentials that need integration in the way they are created by external third parties, while in Europe, Member States primarily look at interoperability from the perspective of their own eID.

This claim of similarities across scale is sustained by the fact that the city of Grosseto has participated very actively in the eID interoperability discussion in several European and global forums, including the Porvoo Group[6] and the Global Collaboration Forum (where it currently serves as acting chair).

4 Open Source to the Salvation

Faced with this daunting task, we committed ourselves to rigorously apply an open source approach to the solution of our problem. The main ingredients include the following:

[6] http://porvoo14.dvla.gov.uk/group.htm l

Engage the Community -- Breaking out of Isolation

The only thing worse than facing tough challenges is facing them alone, and this is not necessary. It was clear from the beginning that the problem we faced could not be solved in isolation. We lacked resources and knowhow, but we possessed the skill of reaching out, of engaging the community, and of communicating —also in an international setting. In Open Source, software and licenses are just the tip of the iceberg and the real essence lies in collaboration and community.

In particular, the person in our ICT department responsible for the development had extensive past experience in collaborating with various open source projects and virtual communities on the Internet. This didn't only include the English language skills that are necessary, but also the skill of finding the right ways and initial contacts that make the difference between finding responses and support or rather being ignored (as it often happens on the mailing lists of open source projects).

Amplify your Knowledge

A key success factor of our project was an elegant and secure design, and thus *knowledge*. The only thing better than knowing something yourself is knowing someone who knows. The knowledge of an individual is necessarily limited, while there are no limits to how many people we can ask.

Even if you are a project manager in a big ICT multi-national, access to key people is always a limiting factor. Even if the corporation has world-renowned experts among their staff, they may be busy on higher priority tasks and unable to dedicate the requested time to you.

This changes drastically when you break out of the “corporate walls”--something that is only possible if you freely share the result of your work with others, hence open source. Now, at least in technical fields, there are top of the line experts out there willing to share their experience and vision. It seems amazing, but who has the skills of collaborating with the community has access to expertise, guidance, review and quality control that even largest corporate environments cannot match. And knowhow often makes all the difference.

Act locally, think globally

Unfortunately, we live in a world of barriers, and success often lies in the ability to break them and reach beyond. Being surrounded by walls and fences, we need to seek windows and gates. Surely, we all believe in networking and we already participate in several established networks. All too often, we stick with our own breed, however, and this is limiting. Local authorities network with local authorities; public organizations exchange experience with other public organizations, and too often we stay within the borders of our language and our culture. Surely, breaking out is not easy, it requires skills that are not always easy to learn; but when we succeed it can make all the difference. These skills are strategic and they increasingly become a success factor for all types of organizations.

Reaching out, our first attempt was naturally to seek out a community of other local authorities who participated in the same pilot project. We have thus organized meetings with the technical people of other municipalities, attempting to incubate open source collaboration, we have set up a national mailing list for the exchange of experience on eIDs and we have had very detailed one-on-one discussions with other local authorities. A key input came from the city of Prato, who had a leading role in the development of their own access control system[7] and we greatly benefited from their experience conveyed in multiple detailed discussions with their key developer.

But breaking out of the box we started to engage global communities, initially those around open source projects like OpenSmartCard[8], mod-python[9], OpenSSL[10], and Apache[11]. The feedback provided by highly knowledgeable people at times to dumb questions was essential to shorten our learning curve, to identify the key concepts and principles, and to understand how to design our system.

[7] that we opted not to re-use for ourselves for both licensing as technical reasons

[8] http://www.opensc-project.org/

[9] http://www.modpython.org/

[10] http://www.openssl.org/

[11] http://httpd.apache.org/

In most cases, the communication used the mailing lists of these projects, and many times the feedback from experts of the projects suggested concrete things to try or requested further information (like detailed error logs) to then identify complete solutions, code changes and additions to solve the problems that we fought with.

We have also found that many key experts on eIDs and eID-access control work with, not surprisingly, national eID projects, often for national governments or major technology providers. We have found access to this community through the Porvoo Group and later also through the eForum PPP eID Working Group and the Global Collaboration Forum on eIDs. Our active collaboration with these groups has been very rewarding and we have since hosted the 12th meeting[12] of the Porvoo Group and serve as European chair of the Global Collaboration Forum.

Participating in these groups has made it possible for our technical responsible to establish personal relationships with key persons of the various eID projects. This has enabled in-depth one-to-one discussions about our work that we presented in the various meetings, identifying problem areas and possible solutions in order to improve our product on the basis of the very extensive practical experience of others who faced similar problems and who had already made mistakes and learned from them.

The Porvoo Group is an informal forum for the exchange of experiences among European eID projects; the Global Collaboration Forum[13] that closely collaborates with Porvoo adds non-European global players, among others the U.S. National Institute of Standards and Technology (NIST[14]) that incorporates the U.S. Government Smartcard Program, the “PIV” eID program for government employees and contractors, and is highly active in international standardization of eIDs at the International Organization for Standardization (ISO).

Participation of our technically responsible person in these forums led to a close contact with the NIST, that led to several visits of key NIST persons to Grosseto and a visit of our representative to the national institute in Gaithersburg, Maryland. Detailed discussions not only gave access to an impressive experience of the institute, but also helped align our work with global strategies and standardization.

The strong rapport with the Porvoo Group and the NIST is currently being consolidated in the Permanent eID Status Observatory (PESO[15]), an informational resource that collects the characteristics of various eIDs worldwide. It is also planned for PESO to use our access control system[16] to demonstrate the interoperability of all eIDs currently issued in Europe and North America.

Breaking out and sharing knowledge and expertise in all Europe and beyond has definitely worked for us.

Be pragmatic – keep it simple

Corporate informatics has become incredibly complex today. Before, and at times instead of, addressing your own problems to be solved, you need to install layer over layer of middleware and libraries, each of which comes with a 500 page manual, has to be configured though a 10 page unreadable XML file, and without the help of an equally complex Integrated Development Environment you can't even think of starting to work… and when something goes wrong there are so many possible points of error that you need to consult a specialist to get your code running. The times when Knuth summarized the essence of Computer Science in a single book and when *small is beautiful* and elegance were guiding principles are evidently over.

While the disease of excessive complexity is surely a fashion of our times, it seems to me that at least some areas of the open source world have remained leaner than the rest of the IT world. Open Source is often very pragmatic, not just because this is a good idea, but out of need, out of lack of resources, and out of the desire to produce tangible, usable results rapidly.

In this spirit, the motto of *simple and it just works* has been our guiding principle and we have indeed managed to work very little, keep our code base very small and maintainable. Software always has bugs -

[12] http://porvoo12.net/
[13] http://www.strategiestm.com/conferences/smart-event/08/global-collaboration-forum.htm
[14] http://csrc.nist.gov/groups/SNS/index.html
[15] http://www.eid-status.info/
[16] TLS-Federation enables the integration of non-certificate credentials such as the Austrian Citizen Card. See http://porvoo14.dvla.gov.uk/documents/tls_federation_final.pdf

complex software has many bugs; to write secure software is very hard - to write secure complex software is impossible.

It may be hard and time consuming to find a simple, elegant and small solution to a problem, but it surely pays in the long run when looking at the whole life cycle of an application that includes maintenance and all the unforeseen extensions and integrations that the future will likely bring.

Reuse—Don't re-invent the wheel

Surely, the simplest way of keeping it simple is to avoid doing anything and instead just reuse what others did. Many reusable components are very mature, tested over a long time by a high number of users, and their long term maintenance comes for free. How could one possibly compete with that with a custom development?

Reuse is one of the core principles of Open Source and *don't re-invent the wheel* is one of the most frequent critiques found in open source forums. Reuse is often not corporate-correct and it may be bad for sales, but in the open source world of free sharing it makes a lot of sense, even more so in the public sector.

So when we started our project, the first step was to look around what others have done in open source. And what we found was the *Belgian Reverse Proxy*[17] by FEDICT[18] (the Belgian Government) that is based on Apache and has contributed all modifications and extensions back to the Apache project. So it was natural for us to start with this existing component, and the discussions with the designer of this component were probably yet more important.

One main area where the Belgian system failed to satisfy all our requirements was eID interoperability. Belgians need to support only their own Belpic eID, while we needed multi-eID support. For this purpose, we wrote a simple Apache handler that knows where different eID issuers write the unique person identifier in the certificate. The handler sets the *remote user* in a consistent way across all eIDs to hide all difference to applications.

For the Porvoo Group *Open Source eID Interoperability Demonstrator* we further extended this approach to map the nationally unique identifiers from the Belgian, Estonian, Finnish, and Italian eIDs into a globally unique name space, thus avoid possible conflicts/collisions of user identifiers. We also added a very simple role-based authorization system in order to make access decisions.

For the *iDEM* project we developed a simple pseudonym creation module to enhance privacy, re-using the concepts developed for the Austrian Citizen Card. Our task in the project was to connect parents with children in municipal schools to remote expert child psychologists in order to get support on how to deal with family problems and get advice on parenting issues. Evidently, these topics are very sensitive and a possible requisite to provide a full name in the forum would likely prohibit any participation. On the other hand, we needed to restrict the service to our own population, and this is decided by full name. We therefore experimented with a pseudonym creation module that lets us make an access decision with a full name but retain full pseudonymity of any participant.

To facilitate use as compared to the Belgian Reverse Proxy we developed a support module in a major application server (an Authenticator for Tomcat) that renders the use of the reverse proxy completely transparent to applications.

The key message is that through smart reuse it is possible to achieve substantial results while limiting new code to an absolute minimum.

Hands off – it has to be secure

Security is difficult. Vulnerabilities are so subtle that they are invisible to the untrained eye. To be really secure requires extensive review of the design by many eyes connected to smart brains, and even more extensive testing of the implementation. Even in software, vulnerabilities are found at times and have to be fixed rapidly by specialists.

[17] http://eid.belgium.be/nl/binaries/REVERSE_PROXY_tcm147-22453.pdf
[18] http://www.fedict.belgium.be/

Developing security software is out of reach for a software developer of a local authority, as it is most likely out of reach for almost any application developer. This is a highly specialized work, and once written it requires review and testing that is even more out of reach. Almost everyone who wants to develop a secure system therefore has to use existing and well-tested components for all security critical tasks.

We thus cover all our security needs with the highly mature implementations of a standard protocol (TLS/SSL) as found out of the box in all major web servers and browsers. Due to its secure design, its relative simplicity and its very large user base the chosen component is likely much more secure than alternative choices that rely on cookies (Liberty Alliance[19], SAML 2.0[20] or one of the various corporate single sign on systems).

5 Where is the system used? Can we use it too?

Thanks to using an open source strategy, we have succeeded in the development of our eID access control system, called *Open Portal Guard*, and it has been in operational use for several months now. While access by citizens to eGovernment services is relatively low, our killer application is the secure access of more than 300 users from other administrations and law enforcement agencies to our population register and other resources.

We are highly interested in many other public and private organizations using our system. This is very likely in Italy, where the general roll-out of our eID is expected to start shortly and more than 8,000 local authorities are expected to issue eIDs and provide services. Considering that the eID roll-out is also taking place or is planned in several other European countries, we expect a high potential of users also at an international level. In its incarnation as Porvoo Group *Open Source Interoperability Demonstrator*, *Open Portal Guard* has already demonstrated that it is applicable to other European situations, supporting the eIDs from Belgium, Estonia and Finland.

In support of dissemination and the creation of a hopefully large user community we are hosting *Open Portal Guard* on IDABC's *Open Source Observatory and Repository* (*OSOR*)[21].

6 Can we steal your tricks?

Successfully applying an open source strategy is not easy. A simple policy decision to do everything in open source from now on is easy but almost worthless - it has to be brought on the ground, and that is not done by decisions, orders or policy. Open source is not a yes or no decision; open source is a path, not a point of arrival. There is nothing black and white about it, no everything or nothing, but just little steps at a time.

The best way of experimenting with open source collaborative development is trying to apply it in one limited area, gathering experience and hopefully opening one's appetite for more. A small experiment is a low-risk undertaking that is much more accessible and realistic than trying to implement some general cover-all decision.

What makes open source happen is its internal capacity and collaboration skill. The easiest way of experimenting in this area is to find a staff member who already is participating in an open source community. This may have gone unnoticed to management or it may be a private hobby after hours… but finding a champion with the right skills renders the path to open source much easier.

Open source skills are acquired very much through *learning by seeing* and *learning by doing*. Therefore, getting others to work with the initial open source champion is the best way for spreading the culture and skill of open source within an organization.

In some areas of life, cheating and getting it the cheap way is particularly difficult—and open source in particular favours honesty and modesty, success through hard work, persistence, and a fair share of suffering. But once achieved tangible results, these are all the more rewarding and of the kind that hardly any other method could have delivered.

[19] http://www.projectliberty.org/

[20] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[21] http://forge.osor.eu/projects/opg/

The critical success factors for engaging the global open source community include the following:

- at least one internal champion with the necessary language skills and experience in being an active member of a community;
- a clear up-front decision to give everything that is created with the help of the community back to the community. This is a prerequisite for others to invest their own resources to solve your problem. Quite often, this decision is expressed in a choice of an open source license;
- successful open source development incorporates a significant percentage of community, i.e., third party, contributions. Planning what autonomous external players do is all but impossible. Therefore, management has to acknowledge that community-based development inherently incorporates risk and uncertainty. It is important to void futile attempts of applying water-fall management approaches. Much rather, it is advised to limit the risk by experimenting in a small area with few resources and possibly by a stage-gate management approach that intervenes when things go wrong before too many resources are spent.

References

Bruegger, B.P, Hühnlein. D. and Schwenk, J. (2008): TLS-Federation - a Secure and Relying-Party-Friendly Approach for Federated Identity Management, in A. Brömme & al. (Hrsg.), Tagungsband „BIOSIG 2008: Biometrics and Electronic Signatures“, GI-Edition Lecture Notes in Informatics (LNI) 137, 2008, SS. 93-104, Extended Abstract available at http://www.ecsec.de/pub/2008_BIOSIG_TLS-Federation.pdf, Full paper available at http://porvoo14.dvla.gov.uk/documents/tls_federation_final.pdf

Stern, M. (2004), Belgian eID Authentication Reverse Proxy User's Guide, Available at http://eid.belgium.be/nl/binaries/REVERSE_PROXY_tcm147-22453.pdf

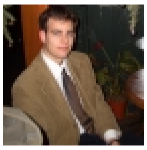
Author

Bud P. Bruegger
Security architect
Municipality of Grosseto, Italy
bud@comune.grosseto.it
http://www.epractice.eu/people/2750

Healthcare Professionals Identification at regional and local level: an RFId integrated scenario based on synergic experiences

Elena Sini
Fondazione IRCCS, Italian National Cancer Institute

Paolo Locatelli



Nicola Restifo

Michele Torresani

Fondazione Politecnico di Milano, Italy

Keywords

RFId, Radio frequency identification, Authentication platform, Identity management, Healthcare, smart card, Regional Healthcare Information System, National Card of Services, Transfusion safety, CRS-SISS

This paper presents a perspective scenario which ties closely a couple of top tier projects related to identification provisioning and traceability developed in the Lombardy Region, Italy.

The Regional Government of Lombardy is promoting an important renewal of the regional healthcare information system, as well as of the IT portfolio in local organizations. The aim is to digitalize processes and data regarding healthcare services in order to improve controlling capabilities, integration among institutions and completeness of information. This will enable new services to citizens and foster cost-effectiveness of care. The new Regional Healthcare Smart Card is a key element: it is a contact card which enables secure electronic identification and access to the new regional healthcare platform. Citizens/patients can access to online services and care providers, pay for analysis, state their social security number and basic medical data. Healthcare professionals and GPs can now digitally sign reports and documents, get access to patients' data from other hospitals, and so on.

In Milan, the Fondazione Istituto Nazionale dei Tumori (the Italian National Cancer Institute), is promoting together with Fondazione Politecnico di Milano and other Institutions a platform for safety and traceability of clinical processes (e.g. transfusions, chemotherapy, medical devices, tissue bank operations) based on Radio Frequency Identification (RFId) technology. Organizations are moving towards RFId in many clinical areas.

Knowing that the Regional Government is exploring scenarios of RFId evolution of the actual contact cards, we have outlined a scenario in which the Istituto could perform an early assessment of the effectiveness of RFId in staff identification and access to clinical applications. The use of a sole card with certified data could solve emerging issues related for example to multiple-provisioning of secure staff identification means, considering the spreading of RFId applications in healthcare. Besides, this could be a chance to enhance overall platform capabilities and move towards and effective system to provide also mobile applications with reliable information on users' identity.

> “ Technologies should help staff into the day-by-day operations, but often increase the complexity of the working environment “

1 Introduction

This paper presents a perspective scenario of synergy on the themes of identification provisioning and traceability, which may bind closely two top tier projects in the Lombardy Region, Italy.

The first is the Regional Social Healthcare Information System (SISS) and its Regional Smart Card (CRS), a project funded and promoted by the Regional Government of Lombardy. CRS-SISS represents an innovative platform in Italy, which aims at also raising the computerization level of healthcare organizations in Lombardy and integrating healthcare information flows.

On the other hand, "Integrated and Safer Transfusions" is a project led by Fondazione IRCCS Istituto Nazionale dei Tumori, which is the Italian National Cancer Institute in Milan. It aims at improving patient safety and traceability through an integrated flexible RFId-based system, covering the whole transfusion process. This application is now becoming a real platform, spreading across other clinical processes and being extended also to other hospitals in Milan.

This paper presents both projects, analyzing their impact on healthcare organizations, and concentrates on a perspective scenario pro-actively promoted by the Institute: we suggest an early trial of an RFId contact-less Regional Smart Card for clinical staff, compliant to the SISS network, in order to simplify identity management and authentication procedures within the hospital.

2 Innovative CRS-SISS project for changing the Regional Healthcare Organization in Lombardy (Italy)

The CRS-SISS project falls within a wider Information and Communication Technology strategy promoted by the Regional Government which aims at supporting innovation and development in all the industry sectors with local and regional-wide initiatives. Started in 1999, the Regional Social Healthcare Information System (SISS) aims at providing innovative services to citizens, healthcare organizations, public agencies in the Lombardy Region, improving both quality of delivered services and healthcare cost-effectiveness (Donatini et al., 2001; France et al., 2005). The project aims at promoting innovation within public healthcare organizations, supporting them in the adoption of common operational guidelines, in the achievement of a certain level of basic IT infrastructure, in the starting of modernization in managerial practice. To exploit the potential of such interventions to higher goals it was necessary to build a regional informative system which is open, modular and flexible, enabling the digital inter-connection of all roles and systems involved in healthcare processes.

SISS development has proceeded by a pilot project approach, followed by further extensions of the system both in geographic coverage and active features. The system was first implemented in April 2007 as a small impact project in a specific area near the town of Lecco. Now the network involves 9,200,000 citizens, 47,000 healthcare professionals, 5,600 general medicine professionals (GPs) and pediatricians (70% of the total), 2,480 pharmacies (97%), 175 public and 4 private healthcare organizations (the latter were allowed to join the network only in 2007).

SISS extranet is an essential lever for enabling the delivery of all new healthcare services and represents the way of networking all actors in the healthcare regional system. On the other side, these have to develop their hospital information systems and make them compliant with the network's protocols and the regional informative needs. In fact, digitalization, integration and tracking of the information flow among healthcare organizations, medicine professionals and other actors over the regional territory will also enable the Government to improve its management capabilities over the regional healthcare budget.

2.1 Major services provided by CRS-SISS

CRS-SISS enables the regional government to improve process awareness and control over care quality. Traceability of treatments, prescriptions, drugs and more over of whole process is granted by a central log system, which traces each significant event. This works because each workstation in the local hospital information systems requires unambiguous identification by logging into the platform before accessing network services (i.e. for viewing patient's file or sign a medical report). The same when patients access for any reason a public healthcare provider: they need to be identified within the regional system.

At the base of CRS-SISS network there are some key services:

- The core is represented by the Regional Healthcare Smart Card (CRS), available both in citizen- and operator-version. This enables first of all safe eIdentification, as it is issued by the regional government and clinical data can be updated only by certified GPs and healthcare providers. Data security within the network and at each access point is granted by a centralized identification management procedure.

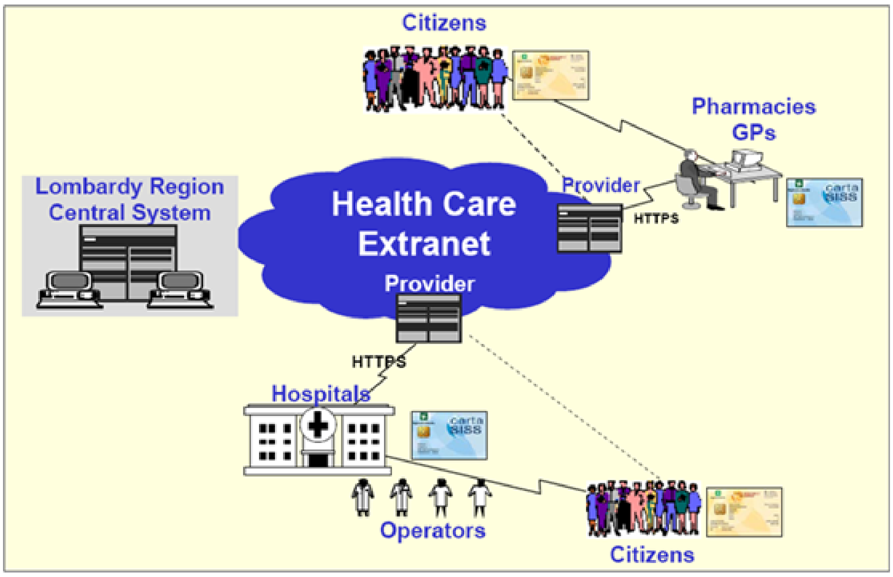


Figure 1 : CRS-SISS Regional Social Healthcare Information System Infrastructure – Schema of the Health Care Extranet (Source: www.crs.lombardia.it)

- Document digitalization and management are a fundamental purpose of the SISS project in order to support the whole healthcare process. The need to confer legal value to digitally-issued reports and system entries is key in order to enable paperless care. Strong digital signature capabilities are foreseen for all healthcare professionals, both in public or in private organizations, all GPs, and certified employees in pharmacies.
- Prescriptions of drugs and services are electronically issued in hospitals and GPs offices with digital signature and central notification. All citizens in Lombardy are enabled to check-in their prescriptions at providers' offices and pharmacies by scanning the prescription sheet and their SmartCard. This is enabled by a common coding reference and a shared citizens database. Over 48 millions of prescriptions have already been provided through the SISS network (May 2007).
- Outpatient booking service is provided through a unique regional call center and also a software used by the general medicine professionals (GPs) and pharmacies. This booking system is extended to certified healthcare providers involved in the regional project. Thus, citizens can book specialist services without having to visit the healthcare providers.
- Reports issuing and management activities are in charge of the healthcare organization providing the service, which has to store them in a SISS-dedicated repository within the hospital information system. Each patient owns information and reports, therefore he has the right to give access permissions to his medical history within the network, at each single clinical episode as well as at a high level, administrating the account through the SISS WebPortal. Thus, patient privacy is assured. Outpatient/First Aid examination reports, examinations results and letters of discharge can now be displayed remotely and imported in the GP's patient record. 6.3 millions of medical reports have been published on the SISS network (May 2007).

The project implements a Virtual Private Network (VPN) and standard communication protocols, which enable to connect safely even if the transmissions take place in a public network. This choice was guided by the need to be able to connect a wide number of users, in theory corresponding to all healthcare caregivers and potentially to all citizens.

The SISS network is based on a three-level hierarchy, where the central domain collects and manages information and makes it accessible to the final users (hospitals, specialists, pediatricians, etc…) through an in-between interoperability and connectivity provider level called Integrated Management Center. More information on interventions to perform on the HIS are described in Section 3.

The flow of information about clinical and administrative matters is linked by a central data log, collecting all links to relevant events and medical reports coming from each local SISS-dedicated-repository. In the future these functionalities will enable to establish an Electronic Patient Folder system for all citizens in Lombardy (Chauldry et al., 2006).

Several benefits can be ascribed to the SISS network implementation: citizens access to social and healthcare services in a more simple way; care services become more controlled and effective, with advantages for healthcare professionals and organizations; the regional government can improve knowledge on processes and organizations of the territory and manage the healthcare budget with more efficiency.

2.2 The Regional Card of Services (CRS) and its key role within the SISS network

The key element of whole CRS-SISS infrastructure is represented by the CRS smart card: the physical key to access the platform. There are two kinds of cards.

The Operator’s smart card enables healthcare professionals to access to SISS functionalities and to sign their entries. Depending on the kind of entries and documents, regional regulations allow the use of an electronic ‘simple’ signature (verifying the operator’s data stored in the chip) or a digital ‘strong’ signature, where the operator also has to digit a personal PIN[1]. The latter is usually applied for reports and certificates, and is a starting point to promote an effective digitalization process within Public Administration and particularly in the Healthcare sector.

The Citizen’s CRS smart card is necessary for patients to access to healthcare services (treatment prescription, patient admission, etc.). Citizen’s cards are also enabled for ‘light’ electronic signature of documents (e.g. written consent forms).

All citizens and healthcare workers (physicians, nurses, qualifying physicians) living in Lombardy have been provided a Regional Smart Card: within March 2007 55,000 operator (approximately 90% of public organizations) and 9,200,000 citizen-smart cards (100%) were issued and distributed. Since November 1st, 2007 citizens in Lombardy have to exhibit their own card in order to access healthcare services provided by the GPs and providers operating within the Italian National Health Service. The card can also be used at home by citizens, who can log into the SISS network through an USB plug-and-play reader and access online eGovernment and eHealth services, like online communication of data to public offices, choice of the personal GP, and so on.

The CRS smart card and SISS network together enable Government to a centralized and effective tracking and monitoring of medical prescriptions, drugs demand, administrative information and other healthcare services provided. The CRS Regional Card of Services replaces all other identification papers. Through this digital device the Lombardy Government aims to identify unambiguously both patients and medical staff everywhere within the region. The CRS smart card complies with the National Card of Services standard, promoted by the Italian Government as an integrated device for citizen identification in public services, but still not physically implemented throughout the country. In fact, in late 2008 the Region of Lombardy agreed with the Ministro della Funzione Pubblica[2] that the CRS card will be the model on which the National Card of Services will be developed and spread to Italian citizens, together with new nation-wide eGovernment services (e.g. online tax declaration, access to public transport services, access to online services by public administration offices ..). This will also lead to widespread and merge many success pilot programs started in other regions of the country.

At this point the CRS is a contact card, with patient/operator identification keys bar-coded and stored in an embedded chip. This chip is also responsible for the calculations related to digital signature. It has been

[1] Of course, all transactions require former system login through username and password in order to access the hospital information system, departmental applications, the Electronic Patient Record.

[2] This is the Ministry responsible for organizing and ruling Italian public administration offices. Thus, it is also the Ministry responsible for eGovernment and eInclusion projects at National level in Italy.

announced that an internal study of the regional government is exploring scenarios of evolution of the CRS card based on other innovative technologies, like Radio Frequency Identification (RFId)[3].

Technology innovation like a RFId evolution of the CRS smart cards could improve pervasiveness and effectiveness of the regional project through the extension of SISS functionalities. RFId technology represents an innovative change lever, which many healthcare organizations have implemented in order to improve process safety and controlling capabilities (Osservatorio RFId, 2007). Usability of RFId smart cards is higher than for the barcode or chip-based ones because RFId technology is contact less and does not require direct physical access to the card. This enables massive scan (e.g. of pallets or boxes), and also excludes problems related to scratch and dirt of barcode labels, as well as those related to fatigue of mechanical parts on optic readers. Moreover, RFId is appreciated because tags can store a much higher amount of data, which can be eventually updated incrementally at each step of the process.

The application of this technology is still at an experimental stage, especially in non-manufacturing processes: thus counting a growth both in new pilot and executive systems, characterized by a reduced number of functionalities (compared to the potential range of achievable support), narrow process coverage and low pervasiveness in process activities. In Europe, mayor concerns are focused on one side on the complexity of implementing pervasively the technology into processes, and on the other side on the privacy of the data stored and the lack of proper regulatory standards and guidelines (RAND, 2008). The use of RFId is now spreading within the healthcare sector, i.e. in form of pilots for traceability and identification purposes (Osservatorio Mobile&Wireless Business, 2007).

We will now describe the potentially strong innovative role of a hospital in the CRS-SISS regional system. On one hand this could be the chance to move towards a more effective infrastructure, moving also certified regional identification provisioning to this modern technology. On the other hand, such a step could finally provide a growing number of new custom applications based of Mobile & Wireless Technology with reliable information on users' identity and allowing them to digitally sign their entries.

3 The Italian National Cancer Institute

Founded in 1925 the Fondazione Istituto Nazionale dei Tumori (from now on: the Institute) is recognized as a top tier Scientific Research and Treatment Institution. The organization has achieved excellence nationally and internationally in the field of pre-clinical and clinical oncology. Placed in Milan, the Institute is both a healthcare delivery organization, providing general treatment services in its wards, and also a high-level research center focused on cancer analysis and care. The Institute employs approximately 1,900 people, and provides care services for about 14,000 inpatients, 12,000 day-hospital admissions, 900,000 outpatients each year. There is an annual average of 900,000 outpatient treatments and more than 15,000 surgical treatments (including 28 liver transplants).

Since 2008 the Institute's hospital information system is SISS compliant, enabling prescription and acceptance operations, issuing and sharing medical report within the SISS network and providing to all clinical staff digital signature functionalities.

The Institute has chosen Fondazione Politecnico di Milano as a partner for a number of innovative projects on technology and organization. This is an academic institution promoting applied research, education and the dissemination of scientific culture for the Politecnico di Milano Technical University in Milan. Fondazione Politecnico is a research center studying various issues related to Information & Communication Technologies (e.g. Mobile & Wireless, RFId and traceability, electronic patient record, hospital information system integration standards) and also responsible of operating coordination in projects, with a specialized team dedicated to the healthcare sector.

3.1 Impact of the CRS-SISS project

The regional CRS-SISS network represents an all-round renewal action on technology and organization in the regional healthcare environment. This approach translates into a gradual systemic innovation of Healthcare

[3] For general information on RFId technology, see: http://en.wikipedia.org/wiki/Rfid; for detailed information on RFId technology, see: Auto-ID Center, Massachusetts Institute of Technology, http://www.autoidlabs.org/ and The UK Institution of Engineering and Technology, http://www.theiet.org.

Information Systems in order to equalize the different levels of computerization across the Lombardy Region, granting at least a lower bound of technology infrastructure to each public provider.

Specific actions are required in order to achieve SISS compliance, therefore change impact on each healthcare organization depends on the specific technology starting point. This integration process is quite critical for several organizations due to their obsolete or lacking information systems. The integration isn't too invasive, forcing organizations to change their whole software and hardware infrastructure. The SISS network imposes compatibility among components of the Healthcare Information System, supporting application integration and funding the purchase of some certified applications, according to a clear target architectural model of the overall healthcare information system. In fact, the Regional Government allocated special funds for public healthcare providers in order to invest in technology innovation and getting their information systems compliant. In order to spread standardization, the regional government also listed a catalogue of vendors where healthcare organizations and professionals could choose among verified software applications. The real problem, as already mentioned, is to integrate electronic flows between pre-existing obsolete proprietary systems and to force clinicians to use technology for their daily activities (e.g. medical reports issuing).

The Institute started from a legacy system from the early 80s and moved to a state-of-art information system, based on the open standard Health Level Seven (HL7) and completely SISS compliant[4].

The hospital information system components which have to interact with the regional system are:

- Patient central database - contains information about all patients in hospital history;
- SISS Local reporting repository - collects all digital reports digitally signed by healthcare professionals and allows their remote online access via the network;
- Integration Middleware - enables data exchange between hospital information system software modules (e.g. HL7 messaging dispatcher, database synchronization);
- The client-side terminal can be updated to be CRS-SISS compliant, but it is not necessary.

Each organization needs the patient's authentication and authorization in order to access his personal information and medical reports. Nowadays a copy of a medical report is digitally signed by the staff and stored into a second database within the Institute. Joining the SISS network, the Institute has the capability to publish the medical report into the SISS repository and make it potentially accessible to all other healthcare organizations in the Lombardy Region, depending on the patient's authorization.

3.2 Safer transfusions and total traceability in the ward thanks to RFId technology

Transfusion in the ward is a key matter both for nurses and physicians working side-by-side. But as stated in literature, nowadays the critical point is operational error (Murphy et al, 2004).

"Integrated and Safer Transfusions" is a project aiming at improving clinical risk management in the whole transfusion chain at the Institute. The project started in 2005 with a pilot within the Allogenic Bone Marrow Transplantation Unit experimenting a subset of functionalities regarding bedside patient-to-bag crossmatch. This was done together with Fondazione Politecnico to explore the capabilities of this technology in the clinical field and also to identify possible critical aspects (further information available at Sini, 2007; Sini, Locatelli, Restifo, 2008 – 1, 2).

This project was selected among others by the Regional Government of Lombardy and awarded with funding for further growth. The pilot system has been running since 2006, the complete RFId application has been released and has gone online in all wards by the end of 2008, enabling total traceability and monitoring of the whole blood transfusion process and implementing advanced haemovigilance features[5]. From the first months of 2009 even pre-transfusion test tubes will be matched to the patient and tracked. This means that RFId tags will be stuck on blood bags, patient sample tubes and patient wristbands. Staff is provided with extra RFId identification cards and PDAs (with an application developed by the project team) and thus enabled to register patients at their arrival, verify the patient-to-item match, identify at any time patients and

[4] HL7 is the communication standard adopted by the SISS network.

[5] In 2007 at the Istituto 1,343 patients were transfused. Total: 12,277 Bags. Estimated value of supplied bags ~2,4 M .

bags. Also blood tests are going computerized. Each event is tracked by the system and sent to the Transfusion Centre, providing an essential informative feedback which was not available before. The Transfusion Services at the institute can now trace the whole transfusion chain, enhancing its monitoring capability.

The project has also involved another important organization of the Lombardy Region: Niguarda Hospital in Milan[6] (Sini, Locatelli, Restifo, 2008 – 2). The two healthcare structures collaborate to share the RFId application and to spread this technology to improve clinical risk management and patient safety. Niguarda started testing the transfusion application in November 2008 within the Oncology Department (2,730 bags transfused in year 2007). Moreover, the regional government is forcing this project to issue blood-bag-tags which have to be interoperable with other similar projects in Lombardy.

Preliminary estimates done in pilot wards using an extended HFMEA Model for risk assessment (regarding data treatment – DeRosier et al., 2002), have stated that process safety may increase by nearly 64% in the transfusion-execution phase, or by 38% in blood sampling activities. Coherent results were obtained assessing the same process with a FMEA-FMECA Model (Trucco, 2004) focusing on patient safety, service continuity, and blood quality[7].

Moreover, the same system is being developed in order to support other critical clinical processes in oncology care, like tracking chemotherapy, drugs administration and medical devices. This means that RFId applications will soon involve all staff members at the Institute: each physician and nurse will be equipped with a supplementary identification badge with a RFId tag built-in (or stuck on the common staff badge). Duplication of the identification devices (e.g. one bar-coded for entering the Institute and one for logging into RFId applications) implies some complications for clinical staff and also a higher degree of complexity regarding identity management. This is not 100% safe, also because information stored on common staff badges is poor and not verified. But they will be used to access core applications in a number of clinical areas (e.g. the RFId platform). Moreover, these two cards sum to a third identification badge, the CRS operator smart card, in order to enable compliance to the regional healthcare network. This triple method of authentication has to be managed correctly for all of the nearly 800 healthcare professionals working at the Institute.

This scenario suggests there’s both a need of a more lean processes and a chance to develop and test a sole system.

4 Perspective synergy scenarios between the two projects

A common factor between the two projects is the need for unambiguous identification, authentication and traceability of care activities and operators performing them. The information flow related to processes needs to be managed in a secure way, simplifying both operator’s authentication procedure and process monitoring activities.

RFId solutions can be a strong means to reconcile a high degree of safety with a technology that is non-invasive neither for patients nor for the staff. RFId may represent the chance to ensure safety and to implement workflow management rules, bounding health workers to follow embedded procedures. The more

[6] The A.O. Ospedale Maggiore Niguarda “Ca’ Granda” is the leading public hospital in Milan and national centre of excellence, hosting 26 centres of high specialization. It is national reference hospital for emergency events and the only regional point of care qualified to perform any kind of tissue and organ transplant. The Hospital employs 740 physicians and 1,540 nurses, performing 54,000 admissions (both ordinary and Day Hospital) and over 3 millions First Aid Station treatments a year.

[7] Failure Mode, Effects, and Criticality Analysis (FMECA) is an extension of FMEA. Is a procedure for analysis of potential failure modes within a system for classification by severity or determination of the effect of failures on the system/process. It is widely used in manufacturing industries in various phases of the product life cycle and is now increasingly finding use in the service industry. Failure causes are any errors or defects in process, design, or item, especially those that affect the customer, and can be potential or actual. In addition to the basic FMEA, FMECA’s effects analysis refers to studying the consequences of those failures, including a criticality analysis, which is used to chart the probability of failure modes against the severity of their consequences (probability of happening + severity = criticality of consequence). Health care Failure Mode and Effect Analysis (HFMEA) is a derivation of those models, designed for healthcare.

integrated the RFId application is, the greater the benefits of digitalization and information integration. Converging to an integrated authentication system the whole organization should obtain benefits in terms of simplification for both identity management procedures and staff's access/clocking.

Moreover, RFId technology is spreading into several other processes, supporting the operations connected to Tissue Bank operations and tracing relevant parameters to determine tissue quality. Another project is focused on tracing chemotherapy treatments with a RFId application which covers all the process, from the treatment preparation to administration to the patient. On the other hand, the Institute is experimenting identification and access control solutions based on RFId technology within some of its peripheral seats. Some staff moves from there to the central seat, increasing complexity of both authentication procedures and identity management operations.

Parallel to this scenario, the CRS-SISS system is spreading regional-wide into healthcare organizations and also the Institute is adopting solutions and technology to become fully SISS compliant. The CRS smart card will represent a necessary tool for the day-by-day work of clinical staff, in order to access to SISS functionalities like digital signature of medical reports.

All these elements suggest the Institute may be a good test center for an integrated authentication system, which merges RFId features to the SISS network through a single identification device. We outlined a scenario in which the Institute could perform an early assessment of the effectiveness RFId in staff identification and access to clinical applications. The Institute could act as a test center, starting from the transfusion process, to unlock further extensions of the regional project in order to extend the CRS-SISS coverage over the clinical processes. RFId-extended CRS cards will enable to identify the clinical staff with an integrated device within the treatment process, tracing the relevant treatment activities with information certified by the regional government. This scenario could increase the pervasiveness of the SISS platform in order to also include this kind of custom application, and thus supporting widely the whole treatment process.

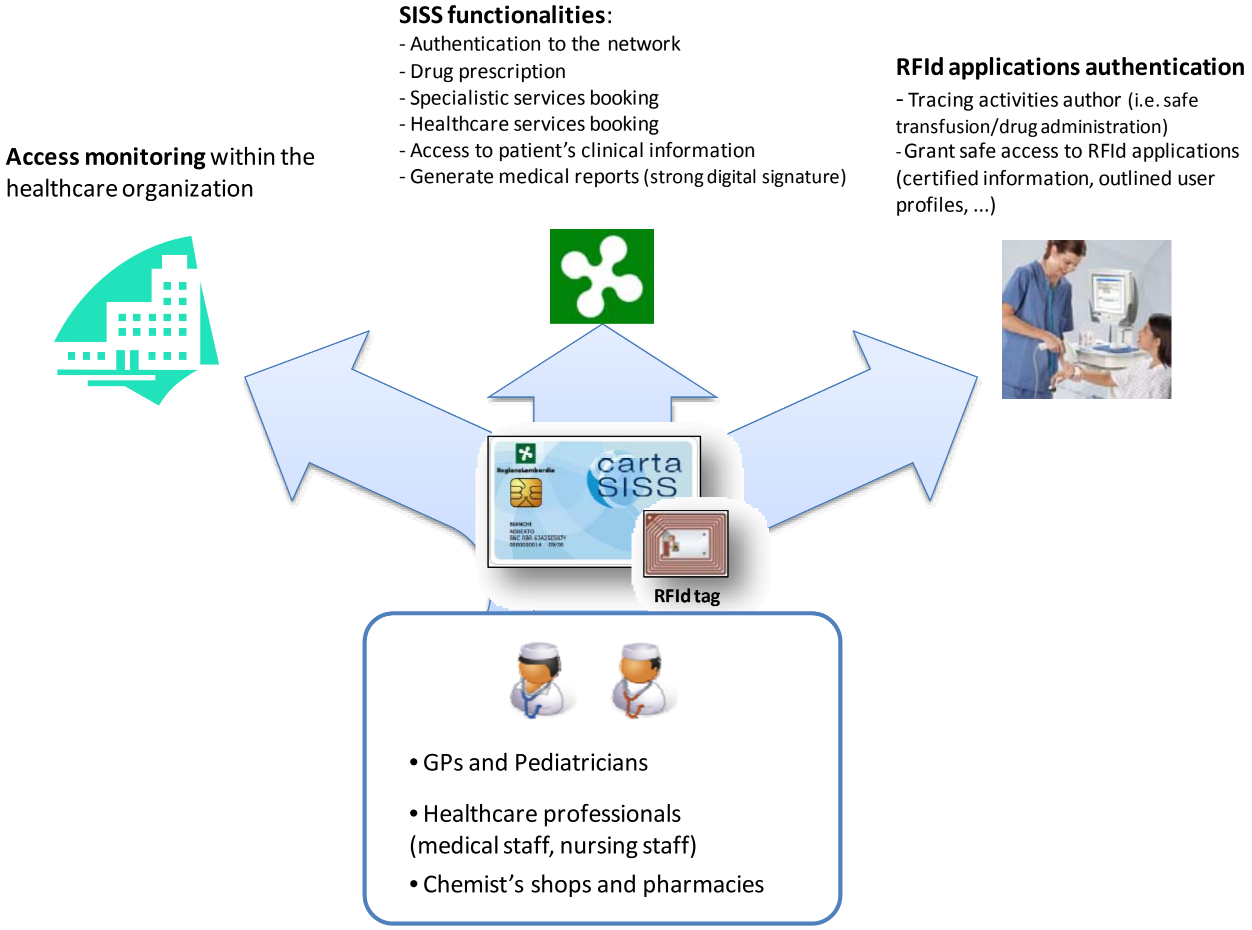

SISS functionalities:
- Authentication to the network
- Drug prescription
- Specialistic services booking
- Healthcare services booking
- Access to patient's clinical information
- Generate medical reports (strong digital signature)
RFId applications authentication
- Tracing activities author (i.e. safe transfusion/drug administration)
- Grant safe access to RFId applications (certified information, outlined user profiles, ...)
Access monitoring within the healthcare organization
carta SISS
RFId tag
• GPs and Pediatricians
• Healthcare professionals (medical staff, nursing staff)
• Chemist's shops and pharmacies

Figure 2: Scenarios of enhancement of the CRS operator card functionalities through the use of RFId.

The complexity of implementing an integrated solution between the CRS-SISS project and the RFId transfusion application suggests proceeding by steps from a smaller pilot to wider implementations with a higher impact. This approach suggests three different scenarios of synergy of increasing complexity, depending on the staff's involvement and pervasiveness within the organization:

- In the first scenario the RFId pilot involves the nursing staff at the Institute (419 people). Benefits resulting from this solution are limited to an increase of process effectiveness, but this solution doesn't simplify the whole authentication system.
- The second phase could involve also the medical staff of the Institute, 323 physicians, adding to a total of 742 people. This scenario moves much more to an integrated solution, unifying the identification and authentication system into a single device for all clinical staff. This simplifying process leads to benefits also for the administrative staff dealing with identity management procedures. Despite this simplification trend, implementing this identification system would need more project management capabilities in order to ensure a successful innovation against critical aspects related to change in habits and procedures.
- The third scenario is the most visionary. It includes a synergy with Niguarda Hospital, which is showing a higher level of computerization than the Institute, but is starting now testing RFId technology for transfusion safety. This would raise the total to 1,063 physicians (740 from Niguarda) and 1,959 nurses (1,540 from Niguarda). Within this scenario the benefits from the synergy can be led to another organization in a similar way. This approach could improve its success if both organizations are able to share their know-how and support each other.

These three scenarios were presented in late 2008 to referees of the CRS-SISS projects, who agreed to open a 'working table' on the subject. Major critical points currently are:

- The alignment of technology standards between local applications and choices made by the region and the central government regarding RFId standards to be chosen for eGovernment applications;
- The provisioning of pilot centers with regional RFId-enabled smart cards[8] fitting both regional and local application requirements;
- The definition of common coding and data handling procedures.

The Italian National Cancer Institute and the Region of Lombardy are going on analyzing in detail application requirements and testing the practical feasibility of the idea. In the meanwhile the institute will further develop its system in order to start the use of ad-hoc RFId smart cards provided by the region for testing purposes. Feedbacks will guide further evolutions.

5 Conclusions

The Regional Government of Lombardy is developing a Social Healthcare Information System (CRS-SISS). At the heart of this project, the new Regional Healthcare Smart Card is a key element: it is a card which enables citizens and operators to secure electronic identification and electronic services. The regional government is currently assessing the opportunity of an RFId evolution of the actual contact smart cards.

The Italian National Cancer Institute in Milan can be considered a forerunner in the usage of RFId in the European hospital sector, as it is moving towards RFId technology in many clinical areas. In this paper we described three likely scenarios of collaboration and synergy between the CRS-SISS project and RFId applications at the Institute and in other hospitals.

Technologies should help staff into the day-by-day operations, but often increase the complexity of the working environment: synergy between RFId technology and the regional smart card is an example of innovation which has a positive impact, both technological and organizational. The use of a sole card with certified identification data could solve emerging issues (i.e. multiple-provisioning of secure staff identification means), considering the spreading of RFId applications in healthcare. Besides, this could be a chance to

[8] CRS cards are currently issued by the Regional Government. From 2010 on, the National Cards of Services project will lead coordination and provisioning activities to the Ministry of Economy.

enhance overall platform capabilities and move towards and effective system to provide also mobile applications with reliable information on users' identity.

This approach demonstrates a possible win-win relationship between two innovation projects, providing benefits for all involved institutions. The prompt feedback by the regional government has proved it - a 'working table' on the subject was opened to evaluate the feasibility of the idea and organize pilot tests.

References

Chauldry, B. et Wang, J. et Wu S. et al (2006). Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care. Annals of Internal Medicine, 144 (10), 742-752

Davenport, T. H. (1993). Process Innovation, Reengineering Work through Information Technology. Boston, Harvard Business School Press

DeRosier, J. et Stalhandske, E. et Bagian, J. et Nudell, T. (2002). Using Health care Failure Mode and Effect Analysis. Journal on Quality Improvement. 27(5), 248-267

Donatini, A. et Rico, A. et D'Ambrosio, M. et Lo Scalzo, A. et Orzella, L. et Cicchetti, A. et Profili, S. (2001). Health Care System in Transition: Italy. Copenhagen, European Observatory on Health Care System

France, G. et Taroni, F. et Donatini, A. (2005). The Italian health-care system. Health Economics, 14, S188-S202

Murphy, M.F. et Kay, J.D.S. (2004). Patient identification: problems and potential solutions. Vox Sanguinis, 87(Suppl.2), S197-S202

Osservatorio Mobile & Wireless Business - School of Management of the Politecnico di Milano (2007). La sfida del cambiamento organizzativo, I risultati del 2007 dell'Osservatorio M&W. Milano: Politecnico di Milano, Dipartimento di Ingegneria Gestionale, retrived November 22, 2007 from www.osservatori.net

Osservatorio RFID - School of Management of the Politecnico di Milano (2007). RFId alla ricerca del valore, I risultati 2007 dell'Osservatorio RFId. Milano: Politecnico di Milano, Dipartimento di Ingegneria Gestionale, retrived June 13, 2007 from www.osservatori.net

RAND (2008). The RAND Europe RFID and Health project team. 2-stage expert panel exercise for a European Commission supported study regarding the most relevant areas, barriers and enablers for the use of Radio Frequency Identification (RFId) technology in the delivery of healthcare. www.rand.org, http://www.rand.org/randeurope/research/surveys/healthcare_rfid/letter.pdf

E. Sini (2007). Project "Safe and integrated transfusion process" - Safe transfusions and total blood traceability in the ward thanks to RFId technology, RFID Outlook "Towards a European Policy on RFID", November 2007, 16, Lisboa

Sini, E. et Locatelli, P. et Restifo, N. (2008). End-to-end safe and efficient clinical processes through an integrated RFId strategy in an healthcare organization. European Journal of ePractice, 2008(2):47-63

Sini, E. et Locatelli, P. et Restifo, N. (2008). Integrated solutions for safer and efficient clinical processes in onchology. WoHiT - The World of Health IT Forum 2008, November 4-6, 2008, Copenhagen, Denmark

Trucco, P. (2004). Strumenti per l'analisi ed il miglioramento della sicurezza del paziente nei processi di cura. Indagine sperimentale sugli effetti in termini di qualità e riduzione dei costi sanitari. , Cod. IReR 2004B037, Final Research Report, IReR Regione Lombardia – Regional Government of Lombardy

Authors

Elena Sini
CIO
Fondazione IRCCS Istituto Nazionale dei Tumori
Elena.Sini@istitutotumori.mi.it
http://www.epractice.eu/people/12813

Paolo Locatelli
Project Manager
Fondazione Politecnico di Milano
locatelli@fondazionepolitecnico.it
http://www.epractice.eu/people/locatelli

Nicola Restifo
Junior Analyst in support to the Area Manager
Fondazione Politecnico di Milano
nicola.restifo@politecnicoinnovazione.it
http://www.epractice.eu/people/nrestifo

Michele Torresani
Graduated in Management Engineering
ICT Department of the Italian National Cancer Institute of Milan
http://www.epractice.eu/people/15050

European Journal of ePractice

The European Journal of ePractice is a peer-reviewed online publication on eTransformation, launched in November 2007. The Journal belongs to the ePractice.eu community, is sponsored by the European Commission as part of its good practice exchange activity and is run by an independent Editorial Board.

The aim of European Journal of ePractice (EjeP) is to reinforce the visibility of articles as well as that of professionals in eTransformation building an author's community which will strengthen the overall ePractice.eu activity. The publication will promote the diffusion and exchange of good practice in eGovernment, eHealth and eInclusion and will be open access, free of charge to all readers. We have a target audience of 50,000 professionals in Europe and beyond, and built on a community of some 13,000 members.

The scope of the European Journal of ePractice reflects the three domains of ePractice.eu: eGovernment, eHealth and eInclusion. We invite professionals, practitioners and academics to submit position papers on research findings, case experiences, challenges and factors contributing to a successful implementation of eGovernment, eHealth or eInclusion services in Europe and beyond.

Read the current calls for papers at www.epracticejournal.eu

Editorial guidelines

– Authors: Researchers and eGovernment practitioners at every level are invited to submit their work to Journal
– Type of material: Articles, case studies and interviews
– Peer-review: The articles are always evaluated by experts in the subject, usually peer-reviewer(s) and member(s) of the portal's Editorial Board
– Length: Full texts of 2,000 - 6,000 words (the word limit may be extended in exceptional cases)
– Language: English

Article structure

1. Title
2. Executive summary of 200-300 words
3. Keywords (3-6 descriptive keywords)
4. Tables, pictures and figures
5. References according to the guidelines
6. Author profile must be made public on ePractice.eu/people

www.epracticejournal.eu
editorial@epractice.eu