MODELING OF EGOVERNMENT BUSINESS PROCESSES ACCORDING TO BPML SPECIFICATION AND ISO 82045 – THE USE CASE OF REQUEST FOR DIGITAL CERTIFICATE

Milan Latinović[1]

Abstract

Public administration institutions focus on constant implementation of new technologies trough separated ICT projects. In most cases, these projects consider simple implementation of ICT technology on current business process without consideration if these processes needs modification in order to accept new technology. Because of this, result might not satisfy end-user needs. This paper proposes approach where processes are first modelled according to BPMN specification and metadata is defined according ISO 82045 standard. Only after this kind of preparation, we can ensure that implementation of ICT technologies will satisfy end user needs. This paper also provides use cases of modelled processes in order to assist anyone who decides to lead ICT projects in this manner.

Keywords: BPML, BPMN, ISO 82045, electronic government, processes, semantics

JEL classification H19

Sažetak

Institucije javne administracije fokusirane su prema stalnoj implementaciji novih informacionih tehnologija putem IKT projekata. U većini slučajeva, ovi projekti podrazumjevaju jednostavnu implementaciju IKT tehnologija na postojeći poslovni proces bez razmatranja da li ovi procesi zahtjevaju modifikaciju prije prihvatanja novih tehnologija. Zbog navedenog, rezultati projekta mogu se pokazati kao neadekvatni za krajnjeg korisnika. Ovaj rad predlaže pristup u kom se prvo vrši modelovanje procesa prema BPMN specifikaciji i definisanje metapodataka prema ISO 82045 standardu. Nakon što se izvrši predložena priprema, moguće je osigurati da će implementacija IKT tehnolo-

1 *mr Milan Latinović, dipl. inž. el* *Agency for Information Society of Republic of Srpska, Banja Luka, Republic of Srpska, Bosnia and Herzegovina* *milan.latinovic@live.com*

gija zadovoljiti potrebe krajnjeg korisnika. Ovaj rad takođe obezbjeđuje slučaj upotrebe na kom se modeluje specifičan poslovni proces sa ciljem pomoći bilo kojoj zainteresovanoj strani koja želi da vodi IKT projekte na predloženi način.

Ključne riječi: *BPML, BPMN, ISO 82045, elektronska vlada, procesi, semantika*

JEL klasifikacija: H19

INTRODUCTION

Public administration institutions constantly implement different information and communication technologies (ICT) inside business processes. Main goal of this implementation is empowering eGovernment services to be more reliable, flexible and transparent and most of all citizen oriented. One of best examples of definition of these goals is Digital Agenda for Europe.

The Digital Agenda for Europe sets eGovernment within a comprehensive set of measures aimed at exploiting the benefits of information and communication technologies (ICT) across Europe. At a time of highly constrained public resources, ICT can help the public sector develop innovative ways of delivering its services to citizens while unleashing efficiencies and driving down costs... [2]

As can be seen Digital Agenda sees eGovernment as a set of measures for improving services to citizens, which essentially means optimizing end user experience, faster and less expensive services, satisfied customer / citizen at the end point. It's easy to realize that ICT won't fulfill this task by itself, but still many of government projects are focused primarily on technology where processes and procedures comes to second place. This practice needs to be changed and there are available tools to do this.

Using the BPMN for defining business processes, in line with ISO 82045, should help notice deficiencies in business processes and help solve them, before the introduction of electronic services. Quality mapping of metadata acts as "connective tissue" for business processes and allows better monitoring of the data inside separated processes as whole.

IMPORTANCE OF DEFINING BUSINESS PROCESSES

When one institution decides to implement new technology or new service it is usually composed of couple of steps: 1) define result; 2) find finances; 3) find implementer; 4) monitor implementation and 5) receive

---

2 *The European eGovernment Action Plan 2011-2015 Harnessing ICT to promote smart, sustainable & innovative Government*, EUROPEAN COMMISSION, Brussels, 15.12.2010

result. Most of the times, institutions lack of adequate preparations for implementer, and this can affect results of activities.

According to previous experiences in revision of ICT projects, mostly related to Registry of ICT projects of Republic of Srpska[3], each institution should be able to provide minimally:

1. Description of current workflows (processes) and procedures;
2. Description of current infrastructure (network schemes, hardware and software infrastructure schemes, databases and data relationships etc.)
3. Description of desired workflows (processes) and procedures; and
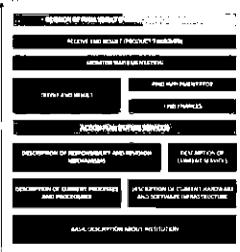4. Description of legislative that affects current and desired workflows.

Figure 2.1. - *Process implementation diagram*

Related to successful product management, Figure 2.1 presents proposed layers of product implementation.

Basic description about institution represents all-important documents about instution, which implements new products, process or service. These documents should contain all-important legal information about institution, should prove that institution is capable of handling desired project, product or service in both legal and capacity terms.

Description of current processes and procedures is important part of preparation documentation. If one institution is not capable of defining current processes and procedures than implementation will be more difficult for realization. Also, if current processes are not described than all lacks and

---

3 *Database on ICT Projects in PA of republic of Srpska – Methodology and Instructions for Forms Filling,* Agency for Information Society of Republic of Srpska, 2009.

bottlenecks will not be recognized in time. In short, lack of current process description will for sure affect future implementation.

Description of current hardware and software infrastructure provides documents about network, servers, storages, capacity usages. Without this documentation, it is not possible to ensure free resources for new product, process or service implementation.

Description of responsibility and revision mechanism represent important part of preparation form implementation, especially in cases where implementer is Government institution. Clear definition of responsibility and revision mechanisms are important when considering eGovernment project implementation.

When talking about current and desired workflows (legacy processes and future desired processes), main problem in describing these is variety of people, services, different professions included in these processes.

At one point, there was a need for finding a common language between different professions and services, so they were able to describe processes in some common way. As answer to these challenges, BPML came into life.

Good definition of BPML: *The Business Process Model and Notation (BPMN) is a standard maintained by the Object Management Group (OMG) and aimed at business analysts and technical developers. BPMN provides a graphical notation that is widely used for process modelling.*[4]

IMPORTANCE OF METADATA AND „DATA JOINTS"

As mentioned in previous section, business process modeling is important, but it is not sufficient for successful project, product or service implementation.

In real life scenario, while completing some procedure or process there will be lots of generated data, in paper or electronic form. This data will include:

* Legal documents and validity providers;
* Demographical documentation;
* Technical documentation;
* Administrative documentation;
* Financial based documentation and finances itself; and
* Any other data that may enter procedure or generate with one.

While having described data, process will also have sets of additional data, mostly on important parts of the system or process (joints), we can call

---

4 C. Natschl¨ager, Towards a BPMN 2.0 Ontology, *Business Process Model and Notation, Third International Workshop,* Lucerne, Switzerland, November 2011, p. 1

this data „data joints". Without this data, process would not be able to handle things such: Where is some document located? When was some document created and by who? Who modified document? Are there any copies of document?

Answers to above questions are contained within so-called metadata.

There are many definitions of metadata. Most of these definitions simply state that metadata is data about data, without any other logical reference, which is not good.

Important thing about metadata is that it is not usable without original (parent) data.

Good and widely scoped definition of metadata:

Metadata is loosely defined as data about data. Though this definition is cute and easy to remember, it is not very precise. Its strength is in recognizing that metadata is data.

As such, metadata can be stored and managed in a database, often called a registry or repository. However, it is impossible to identify metadata just by looking at it. We do not know when data is metadata or just data. Metadata is data that is used to describe other data, so the usage turns it into metadata.[5]

One more important thing is management of metadata itself[6]:

Metadata management refers to the content, structure, and designs necessary to manage the vocabulary and other metadata that describes statistical data, designs, and processes. This includes the development of metadata models to define the content of metadata within some context, building metadata registries to organize the metadata defined in the model, developing statistical terminologies, which define and organize terms into a structure with relationships and identifying the relationships between the terminology structure and other metadata and data.

A. Quantity and quality of metadata

When observing metadata, at some point it is inevitably to think about quantity and quality of this data.

When talking about quantity of metadata it is usual to expect that every issue within a process or procedure will be resolved with adding new metadata fields. At some point, number of these fields expect to increase in high scale. Some good practices about metadata, usage of metadata in document

---

5 Bruce E. Bargmeyer, Daniel W. Gillman, *Metadata Standards and Metadata Registries: An Overview*, Washington, DC 2012, p. 1
6 Bruce E. Bargmeyer, Daniel W. Gillman, *Metadata Standards and Metadata Registries: An Overview*, Washington, opt. cit.

management systems (DMS) and proposed types of metadata are located within ISO 82045.

B. ISO 82045

According to Document Management – Part 1: Principles and methods, ISO 82045 is described as follows:

This standard defines the document concept covering not only traditional paper-based documents, but also, more generally, computer-based information that is identified, structured, processed, controlled and interchanged / communicated as a unit (a closed container of information). [7]

It deals with fixed sets of information with associated metadata and with multiple presentations of these sets of information.

Within this standard, we can find general definitions related to data, metadata, systems etc.; description of principles of document management; proposed metadata for documents with relation to their environment; and metadata associated with activities within the life cycle of a document. Idea is to use these proposals while creating metadata proposals for real working system.

USE CASE OF PROCESSES IN EGOVERNMENT OF REPUBLIC OF SRPSKA

A. Request for digital certificates

Related to important processes and procedures inside eGovernment, Request for digital certificates is one that to consider. In practice, Certification Service Provider (CSP) offers several types of digital certificates to end users, in order to help them identify themselves and protect their digital data.
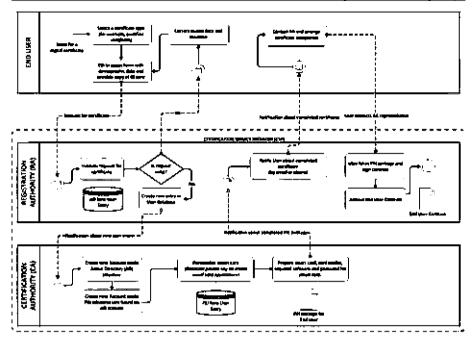
---

7 *ISO 82045-1, Document Management – Part 1: Principles and methods*, CEI/IEC 82045-1:2001, p. 9

Figure 4.1 – *Business process diagram - Request for digital certificate*

Users most often request for qualified certificate, which proves their identity without any doubt. Complicated technical procedures, cryptography and Public Key Infrastructure (PKI) ensure this. All of this is done in line with current regulations. In case of Republic of Srpska, that legislation is consisted of:

- Law on Electronic Document of Republic of Srpska;
- The Law on Electronic Signature of the Republic of Srpska;
- The Law on Electronic Business of Republic of Srpska;
- Regulation on electronic certification holders;
- Ordinance on the records of the certification body;
- Ordinance on measures to protect electronic signatures and qualified electronic signature, lowest amount of compulsory insurance and the application of organizational and technical measures of protection certificates;
- Ordinance on the content and manner of keeping the register of certification bodies for issuing qualified electronic certificates and
- Regulation on technical regulations for ensuring the connection between records of issued and revoked certification bodies in the Republic of Srpska.[8]

---

8 M. Latinović, S. Rajčević, S. Marić, *PKI Systems, Directives, Standards and National Legislation*, Infoteh

As presented at Figure 4.1 Request for digital certificate is not very complex process, but it requires good coordination and „working discipline", in order to deliver final product and maintain satisfied end user.

Request for digital certificates has three instances included: certification authority (CA), registration authority (RA) and end user. Simplified, end user request for digital certificate from RA. This authority examines documentation, and forwards it to CA, which creates product and delivers it to RA. After this RA contacts end user, delivers product, handle legal and other documentation, finalizes process and archive everything.

It is clearly visible that presented process has couple of important data joints:

- Request for certificate (documentation + copy of ID card);
- Notification from RA to CA about new user;
- *AD New User Entry*;
- *PKI New User Entry*;
- Delivery of PKI package from RA to CA;
- Signing contract between RA and end user; and
- Archive End User Contract.

AD New User Entry and PKI New User Entry and being handling by specialized parts of software, which cannot be affected in terms of metadata, so it want be considered. All other data joints are applicable for metadata, and handled in that manner. According to ISO 82045, there are predefined proposed metadata. Idea is to attach significant metadata to data joints of our system.

Data for **Request for certificate** should minimally have this set of metadata:

- *DocumentIdDomainId* - Identifier for a document identification, this will be ID of PKI system inside global AIDRS system.
- *DocumentId* – This will be primary key of specific request.
- *DocumentVersionId* – In cases where end user has to make corrections on request, we will have new versions of these documents, and keep old ones archived.
- *DocumentIdCustomer** - Since all digital certificates are linked to some institution, this will be ID of institution for which end user is working.
- *DocumentIdSupplier** - This will be ID of end user, linked to its profile within system.
- *Title* - Short clear text description of the content of the document.
- *Keywords* – Current DMS of AIDRS has specific protocol related to tagging of documents. These keywords should match tags from DMS.

- *RevisionText* – Description of reasons why RA did not accept request in first place.
- *Status* – Approved, Rejected or Returned for corrections
- *Person* – Identity of the person who affected the status (this is person from RA)
- *CreateDate* - Date when request is/was submitted
- *ExpireDate* – Each request should handle within 15 days, according to legislation.
- *SecurityLevel* – These levels should map according the current legislative [9] [10]

Data for **Notification from RA to CA about new user** should minimally have this set of metadata:
- *DocumentIdDomainId* - Identifier for a document identification, this will be ID of PKI system inside global AIDRS system.
- *DocumentId* – This will be primary key of specific notification.
- *CreatorName* – This will be the name of person who created notification
- *EffectiveDate* – Date when notification became active / important for process.
- *ExpireDate* – Date until CA has chance to formally accept notification and start working on its part of procedure.

Data for **Delivery of PKI package from RA to CA** should minimally have this set of metadata:
- *DocumentIdDomainId* - Identifier for a document identification, this will be ID of PKI system inside global AIDRS system.
- *DocumentId* – This will be primary key of specific delivery.
- *CreatorName* – This will be the name of person who created PKI package and delivered it to RA
- *EffectiveDate* – Date when package was created (not sent, or delivered)
- *Title* - Short clear text description of the content of the delivery.
- *Person* – Identity of the person who created PKI package and delivered it (same person)
- *SecurityLevel* – These levels should map according the current legislative [7] [8].

Data for **Signing contract between RA and End User** should minimally have this set of metadata:

---

9 Law on Information Security, Official Gazette of Republic of Srpska, 70/11 (In Serbian)

10 *Regulation on Standards for information security*, Official Gazette of Republic of Srpska, 91/12 (In Serbian)

- *DocumentIdDomainId* - Identifier for a document identification, this will be ID of PKI system inside global AIDRS system.
- *DocumentId* – This will be primary key of specific delivery.
- *CreatorName* – Name of the person who created contract
- *Person* – Identity of the person who signed contract (end user)
- *EffectiveDate* – Date when Person signed contract and took over PKI package. This is very important part of metadata, since from this moment digital certificate considers as active and valid.
- *SecurityLevel* – These levels should map according the current legislative [7] [8].
- *ReferedDocumentId* – This could actually be an Array of values pointing to additional documents such as ID card or request for certificate etc.

CONCLUSION

This paper describes modeling of eGovernment business processes according to BPML specification and ISO 82045. As described at the beginning of this paper, careful planning of process and procedure for any eGovernment service needed in order to provide high quality service.

This paper provided full example of handling eGovernment process, use case of Request for Digital Certificate, trough BPML schema definition, proposal for data joints and metadata for these joints. In addition, this paper proposed creation of data joint aggregator with markers required for workflow tracking.

Proposed use case can review as full plan for process and service integration according to Figure 2.1 As proposed in main hypothesis of this paper, presented usage of BPML and ISO 82045 is mandatory preparation for insurance of successful software (in some cases even hardware) implementation of ICT project, process, procedure or service.

This paper should be consider as good service developing practice, and described use case may even be considered as prove of concept which can be used by any future eGovernment stakeholders and implementers.

REFERENCES

1. *The European eGovernment Action Plan 2011-2015 Harnessing ICT to promote smart, sustainable & innovative Government*, EUROPEAN COMMISSION, Brussels, 15.12.2010
2. *Database on ICT Projects in PA of republic of Srpska – Methodology and Instructions for Forms Filling*, Agency for Information Society of Republic of Srpska, 2009. (In Serbian)
3. C. Natschl¨ager, Towards a BPMN 2.0 Ontology, *Business Process Model and Notation, Third International Workshop*, Lucerne, Switzerland, November 2011, p. 1
4. Bruce E. Bargmeyer, Daniel W. Gillman, *Metadata Standards and Metadata Registries: An Overview*, Washington, DC 2012, p. 1
5. *ISO 82045-1, Document Management – Part 1: Principles and methods*, CEI/IEC 82045-1:2001, p. 9
6. M. Latinović, S. Rajčević, S. Marić, *PKI Systems, Directives, Standards and National Legislation*, Infoteh Jahorina, Republic Of Srpska, 2010. (In Serbian)
7. *Law on Information Security*, Official Gazette of Republic of Srpska, 70/11 (In Serbian)
8. *Regulation on Standards for information security*, Official Gazette of Republic of Srpska, 91/12 (In Serbian)