RESEARCH IN LOGISTICS & PRODUCTION

USING RFID TECHNOLOGY FOR ADMINISTRATIVE OFFICE WORK ORGANIZATION

Maciej Kiedrowicz*, Tadeusz Nowicki** and Robert Waszkowski***

Cybernetics Faculty, Military University of Technology, 00-908 Warsaw,
Kaliskiego 2 Street, Poland,
*Email: tnowicki@wat.edu.pl
**Email: rwaszkowski@wat.edu.pl
***Email: mkiedrowicz@wat.edu.pl

Abstract The paper presents procedures performed in the administrative office processing open and secret documents. It is assumed that office is equipped with devices and software for automatic identification documents based on RFID tags. Office procedures have been presented in the form of business processes in BPMN.

Paper type: Research Paper

Published online: 16 July 2016
Vol. 6, No. 3, pp. 245-257
DOI: 10.21008/j.2083-4950.2016.6.3.5

ISSN 2083-4942 (Print)
ISSN 2083-4950 (Online)

Keywords: *RFID, BPMN, administrative office, business processes, document identification, Aurea BPM*

1. INTRODUCTION

The second decade of the twenty-first century is a time of increasingly widespread use of electronic documents. Electronic applications, certificates and invoices have become a natural part of reality in Polish enterprises.

However, paper documents remain of great importance. Agreements, certificates, securities, deeds, records of employees are some of examples of documents stored in paper form. Storage and archiving of such documents, as well as manage access to them is a challenge and very often requires the use of certain procedures supported by IT systems.

Offices of modern enterprises are equipped with hardware and software to effectively manage open and classified documents. Complementing the currently used solutions with the opportunity to identify each document using RFID tags makes possible to obtain an automated document management system. This gives great opportunities in the field of document security, accountability and traceability.

This paper presents the procedures the restricted access administrative office equipped with RFID readers placed in cabinets, desks and entrance sluices. By using these readers, it is possible to automatically and immediately read the content of cabinets, identify documents on the desk and register facts of entry or exit of the document. Taking into account such innovative technological capabilities, the new business processes of the administrative office were proposed.

2. BUSINESS PROCESSES OF THE RFID EQUIPPED RESTRICTED ACCESS ADMINISTRATIVE OFFICE

The business process map of the processes selected during the analysis of the restricted access administrative office work is shown in Figure 1.

1. In the following chapters, the main business processes of restricted access administrative office will be presented in details.

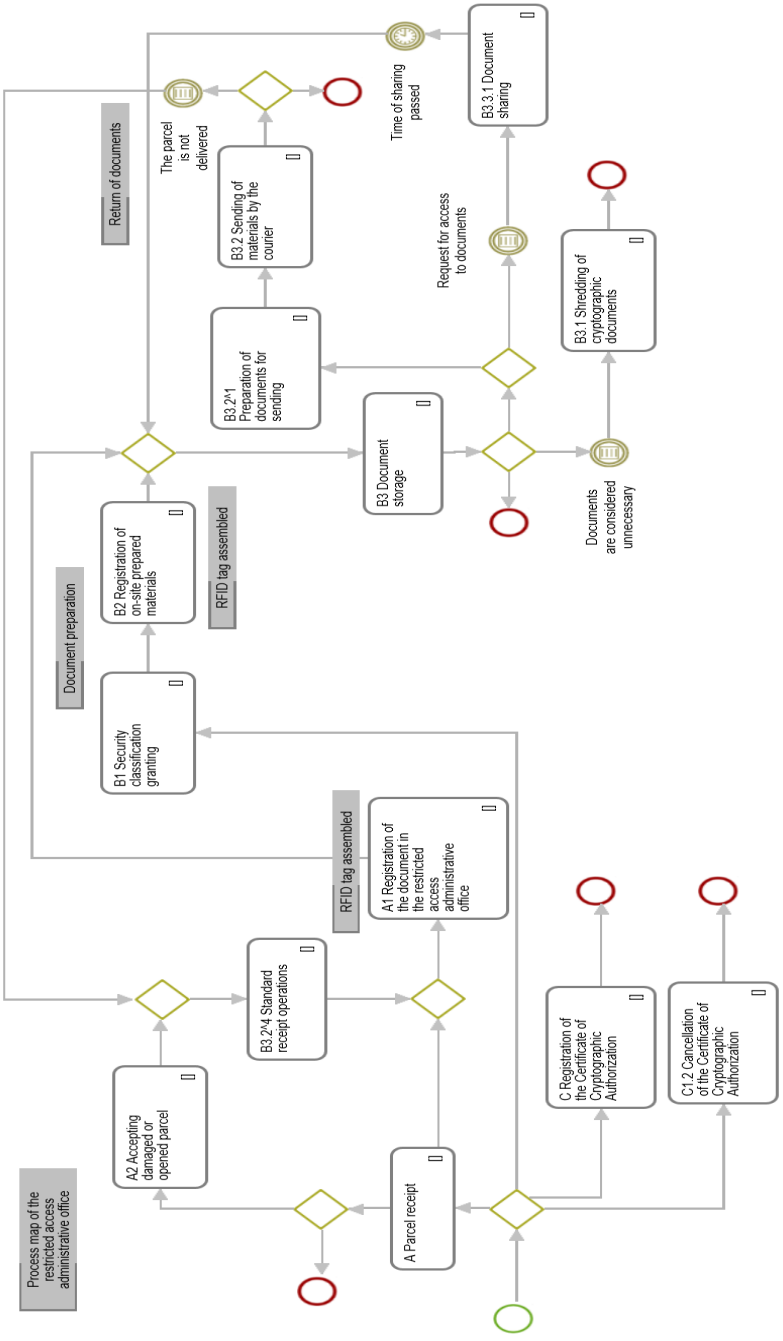

Fig. 1 Business process map of the restricted access administrative office; Source: own elaboration

3. PARCEL RECEIPT BUSINESS PROCESS

The Parcel receipt business process (Fig. 2) is implemented according to the following scenario:

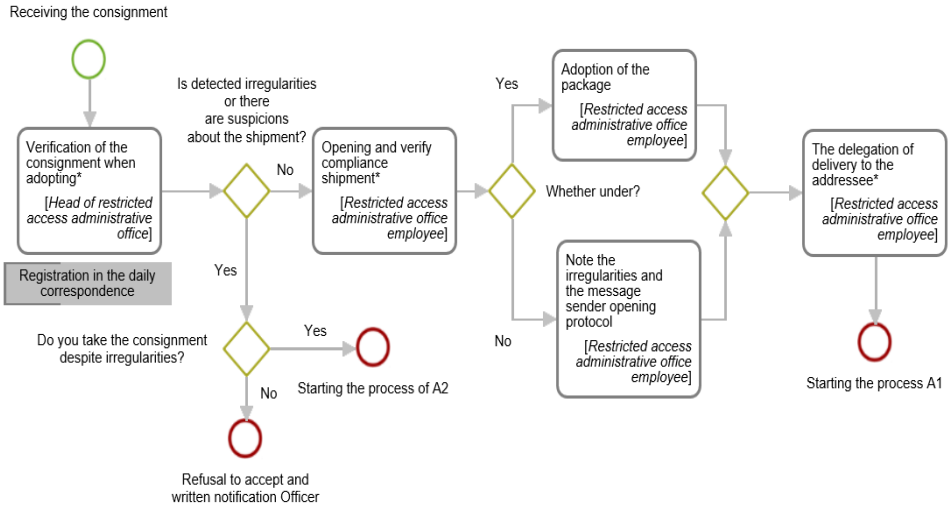

Fig. 2 Parcel receipt; Source: own elaboration

1. The process is initiated at the time of shipment acceptance by an employee of the restricted access administrative office (K), which introduces start-up form the date of acceptance of the consignment and enters the data into the Book of delivery / Schedule shipments issued and approve the task.
2. Then Director receives the consignments and shipment checks on entry. It introduces data on the recipient and sender acknowledges receipt of the shipment, enter data for verifying the compliance of the consignment.
3. The head of the secret office notes if the irregularities were detected during the check or if there are suspicions about the shipment.
    a. If Yes (go to step 4).
    b. If Not (go to step 5).
4. The head of the secret office decides whether to accept the consignment, despite the anomalies:
    a. If not, he refuses to accept the shipment and shall notify in writing the authority. This ends the process.
    b. If yes, it starts the process of "Accepting damaged or opened parcel".
5. The secret office manager hands on the parcel to the secret office employee.
6. The employee opens the parcel.

7. Secret office employee checks the compatibility between the contents of the consignment, and the evidence numbers listed on the inner envelope.
8. The secret office employee verifies the number of pages, attachments and pages of appendices according to the number indicated on the individual cryptographic media.
    a. If he notes the irregularity, he puts entry in the parcel opening register describing the existing irregularities and endorse this fact in the official correspondence. Then he attached the opening confirmation letter to the cryptographic materials. Then he sends the opening confirmation letter to the original parcel sender (go to step 10).
9. Secret office employee accepts the parcel.
10. Secret office employee forwards the parcel to the addressees:
    a. If it is an urgent parcel (go to step 11).
    b. If it is an ordinary parcel office worker may be in no hurry with the transfer of the consignment. Starting the process "Registration of the document in the restricted access administrative office".
11. The secret office employee passes the parcel immediately. He endorses this fact in the notes of the muster apparatus specifying the date and time of delivery. It starts the process "Registration of the document in the restricted access administrative office".

4. BUSINESS PROCESS REGISTRATION OF THE DOCUMENT IN THE RESTRICTED ACCESS ADMINISTRATIVE OFFICE

Business process "Registration of the document in the restricted access administrative office" (Fig. 3) is implemented according to the following scenario:

1. The head office or other authorized employee verifies that the correspondence contains the notation 'by hand':
    a. If Not (go to 2).
    b. If Yes (go to 7).
2. The head office or other authorized employee puts stamp effect on the first page of cryptographic material.
3. The head office or other authorized employee form seal imprints on the annexes.
4. The head office or other authorized employee completes more items official correspondence.
5. Head office or other authorized employee enters on the document the date of registration.
6. Head office or other authorized employee entered on the document items in the Official correspondence. Starting the process of "Document storage".

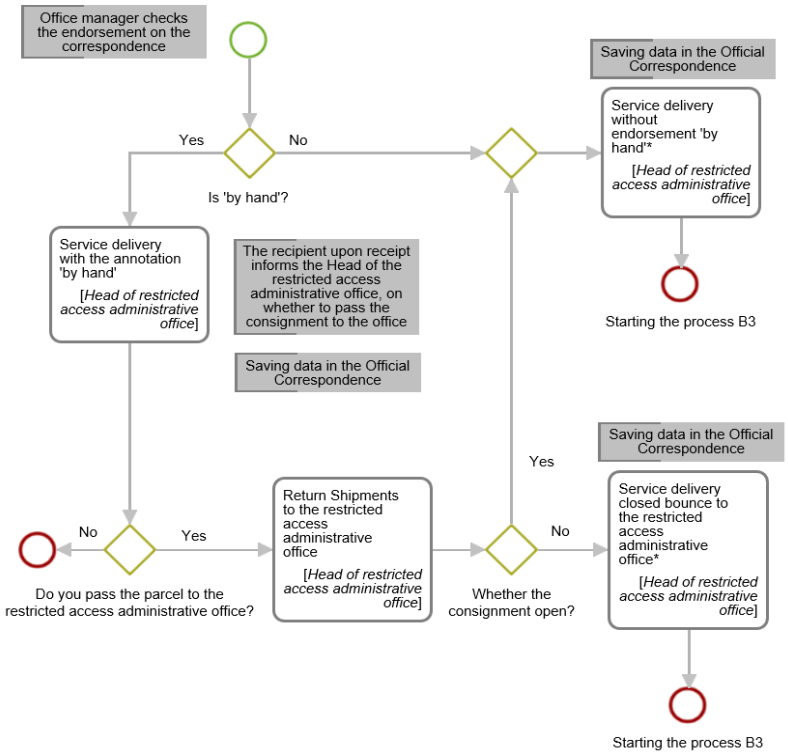

Fig. 3 Registration of the document in the restricted access administrative office; Source: own elaboration

7. Head office or other authorized employee leaves the shipment in a closed inner wrapping.
8. Head Office or other authorized employee fits in the Official correspondence information contained in the inner packaging.
9. Head office or other authorized employee fits in the Official correspondence date of receipt.
10. Head office or other authorized employee shall in section Comments endorsement 'by hand'.
11. Head office or other authorized employee of the stamp imprints impact on consignment.
12. Head office or other authorized employee enters a registration number by the Official correspondence.
13. Head office or other authorized employee shall enter the date impact on consignment.
14. Head office or other authorized employee transfers the load directly to the addressee or person authorized.

15. The recipient or an authorized person decides whether the consignment is transferred back to the office:
    a. If Yes (go to 16).
    b. If Not – end of the process.
16. The recipient or a person authorized returns the parcel to the office:
    a. Parcel opened (go to 2).
    b. Parcel closed (go to 17).
17. Service delivery closed bounce to the office. Head of office or other authorized employee of the stamp imprints round numbers or their names.
18. Head office or other authorized employee notes that the consignment store in the form of sealed package in the "Remarks" Official correspondence. Starting the process of "Document storage".

5. BUSINESS PROCESS 'SECURITY CLASSIFICATION GRANTING'

Business process 'Security classification granting' (Fig. 4) is implemented according to the following scenario:

1. The person responsible for assigning clauses on the start-up form selects the type of material and approve the task:
    a. If a non-electronic document is selected, the task 'Giving the classification of doc. non-electronic' is started. Head of restricted access administration office enters:
        i. On each page (go to 2).
        ii. On the first page (go to 7).
        iii. On the last page of the content (go to 10).
    b. If an electronic document is selected, the task 'Giving the classification of doc. electronic' is started (go to 15).
    c. If other materials are selected, the task 'Giving the classification of other material' is started (go to 24).
    d. If permanently framed collections of documents, books and records are selected, the task 'Giving the security classification' is started (go to 25).
2. Gives security classification at the centre, as the first element in the header and footer.
3. Types the copy number, or, in case of a single copy enters "Single".
4. Enters a letter-digital signature.
5. Enters page numbers and the number of pages in the entire document.
6. Adds additional instruction.
7. Enters the name of the entity or organizational unit.
8. Enters the name of the place and date of signing the document.

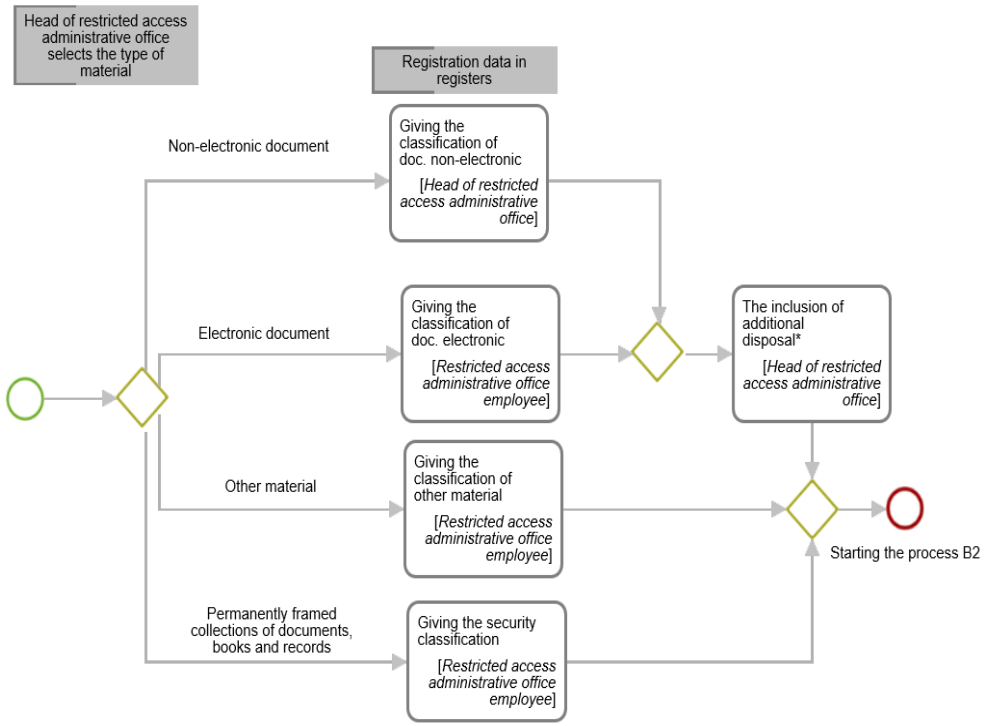

Fig. 4 Security classification granting; Source: own elaboration

9. In the case of a document that has been given a correspondence course, enters name or the name of the recipient.
10. Enters the number of attachments, number of pages.
11. Enters security classification attachments with numbers under which they were registered.
12. Enters position and name of the person authorized to sign it.
13. Enters the number of copies made and recipients of individual copies.
14. Enters the name of the contractor. There is part of the supplementary and then start the process of "registration materials produced".
15. Enters the security classification in the metrics form.
16. Enters a letter-digital signature.
17. Enters the name of the entity or organizational unit.
18. Enters the document registration date.
19. In the case of a document that has been given a correspondence course, your name or the name of the recipient.
20. Enters security classification attachments with numbers under which they were registered.

21. Enters position and name of the person authorized to sign the document
22. Enters name and given name or the sign of the author.
23. Enters the name given to the document, or determine which document relates. There enters the supplementary and then starts the process of "Registration of on-site prepared materials".
24. Enters classification and signature-digit alphanumeric through stamping/ printing/permanent marking on the casing or packaging. Starting the process "Registration of on-site prepared materials ".
25. Enters classification clause on the outer walls of the cover and the title page. Starting the process "Registration of on-site prepared materials".

6. BUSINESS PROCESS 'SHREDDING OF CRYPTOGRAPHIC DOCUMENTS'

Business process 'Shredding of cryptographic documents' (Fig. 5) is implemented according to the following scenario:

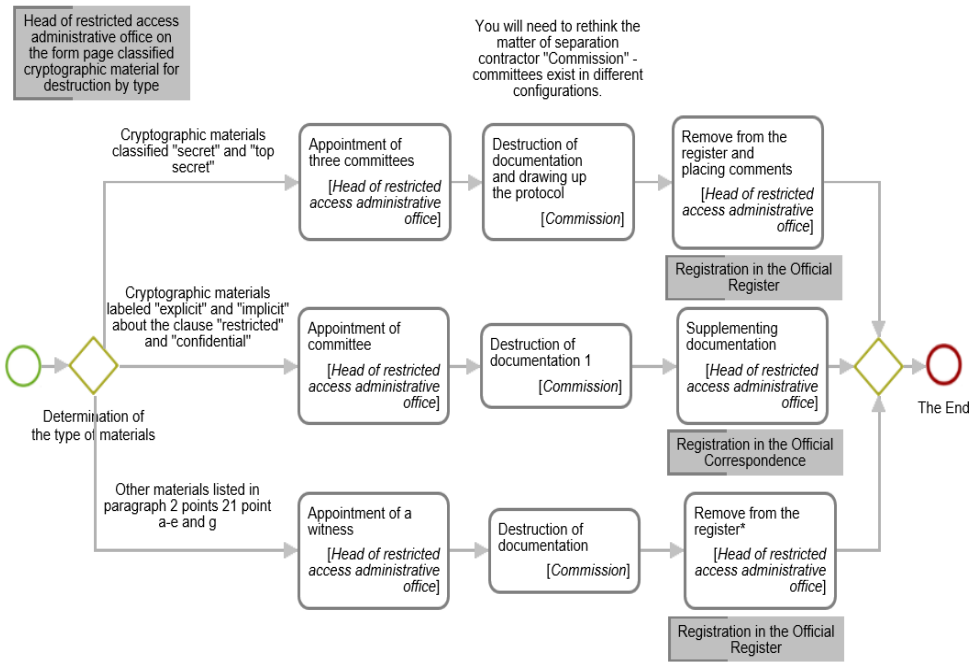

Fig. 5 Shredding of cryptographic documents; Source: own elaboration

1. On the start-up form Head of the office classifies materials to be destroyed by their type (documents stored in computer databases documents are not to be destroyed):
    a. If the cryptographic material classified SECRET and TOP SECRET start the task Appointment of three member commission (go to step 2).
    b. If the cryptographic materials designated as EXPLICIT clause and CLASSIFIED on proprietary and confidential start the task set up a commission (go to step 6).
    c. Other materials: documents cryptographic system components (block module, component and auxiliary cryptographic devices), cryptographic products, publications and cryptographic technical documentation cryptographic systems and products and forms and other registration device to start the task to call a witness (go to 10).
2. Head of organizational unit is appointed, at least 3 person commission.
3. The presence of commission do shred the documentation.
4. The presence of commission to draw up minutes.
5. The manager of an organization is removed from the register by applying comments about this fact. The end of the process.
6. The manager of the organization appoints a committee composed of the office staff person or contractor.
7. The presence of commission to shred of documentation.
8. The manager of the organization enters in the "Remarks" muster apparatus annotation reads: "destroyed by the date …".
9. The manager of an organization completes the date and legible signatures of persons engaged in the destruction of cryptographic materials. The end of the process.
10. The manager of an organization appoints a witness: Deputy Chief Registry Officer or any other person holding a security clearance.
11. The presence of commission destruction of documentation.
12. The manager of an organization confirms the destruction of the form AF 21 PL.
13. The manager of an organization is removed from the register by applying comments about this fact. The end of the process.

7. CONCLUSION

Basic functions of the solution proposed in the research project, is the management of classified and non-classified document flow, the document access control and the supervision of their copying, as well as document access management.

The results of the project will be used in document management systems, used in local organizations, banks, government organizations. These systems store per-

sonal data or corporate data as well as support document flow between different organizations.

The measurable social benefits are also important. Among them worth mentioning is the increased confidence of the third party institutions, like public, government and non-government organizations, cooperating associations, companies and corporations, to state authorities.

Both increasing the security level of documents, as well as raising the security level associated with the persons authorized, will improve the quality of the entire process associated with document flow. A tangible result of these actions will be reduction (eventually the total liquidation) of incidents related to the uncontrolled disclosure of classified documents and data. This has considerable importance from the state safety point of view, resulting even with today's terrorist threats. Poland, as a member of the European Union and NATO, has a duty to keep particular efforts with regard to the protection of the processing of sensitive information.

An additional advantage of the proposed solutions, except providing a better control over the storage and document sharing, will be the ability to trace the document flow between safety zones with a knowledge of authorized persons that have been using the documentation. Mapping of classified documents' flow, in case of incident, will allow the effective investigation of the causes of their occurrence and will allow setting a list of potential perpetrators.

The main users of the system will be units of state administration, including subordinate to the Ministry of National Defence and the Ministry of the Interior. An important field of application for the results of the project will also include the area of justice and health care institutions.

Potential customers interested in deploying the results are the following institutions: Ministry of National Defence, Ministry of Internal Affairs, Internal Security Agency, Foreign Intelligence Agency, National Police and Polish Border Guard.

In addition, the following institutions would be interested in the project results: hospitals, libraries, national archives, colleges, universities.

Despite the increasingly popular use of electronic documents, there are still areas where it is necessary to store paper documents. For example, the whole area of Justice, from the police, prosecutors, to the ordinary and administrative, regional, district and appellate courts uses documents in paper form. In accordance with the Polish and European legislation, most of the paper documents is evidence in police proceedings, prosecution and the court, and, consequently, you cannot convert them to electronic form - must be in its traditional paper form.

Another example of this are various medical records produced by different institutions participating in the healing process. Taking into account the size of the produced medical records, its current storage and backup poses a serious challenge to clinics and hospitals. Also in this area, the use of the results of the project would provide huge benefits thanks to automation of document processing operations.

The national archives, which are part of the public administration, manage documents that are a perpetual source of providing historical society, history of the

Polish nation and of our statehood. The purpose of the state archives today is also to secure archival materials created in the public sector. Application of project in checking archival resource, already at its creation in the institutions that have archival materials, will allow securing historical sources, through supervision and control over the movement of labelled media. Miles and miles of archives collected in different archives (for example, the churches, political parties, etc.) secured and recorded by the system are part of the strategic objectives specified by the Executive Director of the State Archives in the document issued on December 29, 2010 entitled "National Archives Strategy for the period 2010-2020." The use of the project will allow documents to be more effective secure from damage or theft both during its storage and accessing.

The system, based on RFID technology, can be also applied to other institutions, which store archival materials, such as libraries, museums and documentation centres, etc. The library can also use the system for securing individual cards of valuable antique books.

The implementation of the system will contribute to the growth and competitiveness of the sector of workflow systems in Poland. This is due to the fact that advanced solutions, based on the radio, and automatic identification of documents do not exist in Europe. With such technology, Polish institutions and companies, become a leading supplier of solutions for the European market, and later also the worldwide.

ACKNOWLEDGEMENTS

This work was created as a part of project DOBR-BI04/006/l3143/2013 supported by NCR&D.

REFERENCES

Finkenzeller K., (2003), RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition, John Wiley & Sons.

Cole P.H. & Ranasinghe D.C., (2008), Networked RFID Systems and Lightweight Cryptography, Springer.

Zhang Y., Yang L.T. & Chen J., (2009), RFID and Sensor Networks Architectures, Protocols, Security and Integrations, CRC Press.

Paret D., (2009), RFID at Ultra and Super High Frequencies. Theory and application, John Wiley & Sons.

Bolic M., Simplot-Ryl D. & Stojmenovic I., (2010), RFID Systems Research Trends And Challenges, John Wiley & Sons.

Miles S.B., Sarma S.E. & Williams J.R., (2008), RFID Technology and Applications, Cambridge University Press.noFilis “CrossTalk AppCenter 3.0 Installation and Administration Guide”

Canon UniFLOW documentation - www.canon.com

Aurea BPM system documentation - aurea-bpm.com

Braude E.J. & Bernstein M.E., (2011), Software engineering: modern approaches, J. Wiley & Sons.

Larman C., (2012), Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development, 3/e, Pearson Education India.

http://aurea-bpm.com

BIOGRAPHICAL NOTES

Maciej Kiedrowicz is an assistant professor at Cybernetics Faculty, Military University of Technology, Warsaw, Poland. His research interests are connected with database modelling and design, system engineering, business processes modelling and analysis. He is the author and co-author of many academic monographs and scientific publications.

Tadeusz Nowicki is an associate professor at Cybernetics Faculty, Military University of Technology, Warsaw, Poland. His research interests are connected mainly with mathematical modelling, computer simulation, optimization methods, computer systems effectiveness, business processes modelling and analysis. He is the author and co-author of 6 academic monographs and more than 160 scientific publications.

Robert Waszkowski is an assistant professor at Cybernetics Faculty, Military University of Technology, Warsaw, Poland. His research interests are focused on business process analysis, modelling and automation, databases, computer simulation, optimization and project management. He is the author of more than 30 scientific publications. He managed many projects in the field of business process management.