RESEARCH IN LOGISTICS & PRODUCTION

ACCESS CONTROL SYSTEM FOR RFID-TAGGED DOCUMENTS IN SUPPLY CHAIN MANAGEMENT

Tadeusz Nowicki*, Maciej Kiedrowicz*, Robert Waszkowski*, Agata Chodowska** and Agnieszka Lach**

* Cybernetics Faculty, Military University of Technology, 00-908 Warsaw, Kaliskiego 2 Street, Poland, Email: tnowicki@wat.edu.pl
Email: rwaszkowski@wat.edu.pl
** Tecna Sp. z o.o., Warsaw, 01-823, Poland, Kasprowicza 103A/9 Street,
Email: agata.chodowska@tecna.pl
Email: agnieszka.lach@tecna.pl

Abstract: The paper presents the concept and design models of the access control system for RFID-tagged documents in supply chain management. The access control system allows to assign privileges to particular persons or groups of persons for specific documents. When implementing the processes related to the handling of documents, the required privileges are verified. Existence or lack of such privileges affects further development of such processes.

Paper type: Research Paper

Published online: 30 April 2017
Vol. 7, No. 2, pp. 143–157
DOI: 10.21008/j.2083-4950.2017.7.2.7

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

Keywords: *modeling, business process management, business analysis, RFID, access control*

1. INTRODUCTION

In supply chain management, the information exchange process is considered key to managing physical product flow and improving cost and service performance of enterprises (Kee-hung Lai, Wong & Siu Lee Lam, 2015).

For competitive advantages, many companies have now focused more on their supply chains and hence thought of ways to improve their supply chain management. A supply chain stays connected by information flow, finance and material, suppliers, producers, retailers, distributors and customers.

Information sharing in the supply chain may bring a number of benefits to enterprises. For example, the products match the consumer's demand more closely, thus, the market changes may be anticipated. The broad use of advanced information technologies in supply chains, such as Electronic Data Interchange (EDI) and Web technologies, demonstrates that organizations have come to substantiate the importance of integrating information.

Actually, many supply chain-related issues arise due to the lack of sharing information within the members of a supply chain.

Stadtler defines the Supply Chain Management (SCM) as an act of sharing material, information and financial information within organizational units so as to meet the customers' needs and hence strengthen the entire supply chain.

The supply chain may be described as a series of organizations that may be involved in different processes and activities to produce products and services for ultimate customers, both upstream and downstream. Therefore, the supply chain is made up of a number of companies including suppliers, distributions and end-customers.

The supply chain management is aimed at achieving certain objectives, such as improvement of customer satisfaction and service as well as increase of competitiveness. The supply chain management also aims at lowering the costs and resources involved in the creation of products as well as improving their efficiency and effectiveness. SCM also focuses on reducing inventory levels and respective costs, increasing profits and improving cooperation.

The manufacturing sector plays a key role in supporting economic development. To survive in today's global economy, manufacturers definitely need to rethink their approach to cooperation and hence provide ways of sharing current information within various enterprises. However, providing the software and hardware alone is not sufficient. The members should have the willingness to participate in information sharing activities. Nowadays, enterprises do not operate alone; they have now been networked to many other partners.

Information sharing means distributing useful information for systems, people or organizational units. To enhance the results of information sharing, organizations should answer four main questions: First, we ask what to share, then, whom to share it with, how to share, and finally when to share. The quality of answers

will help to avoid redundancy, reduce sharing costs and improve responses. The term ‘Information Sharing’ can also be referred to as the ‘Knowledge Sharing’ or ‘Information Integration’. There exists a myriad of information in the supply chain, such as logistic, business, strategic, tactical and much more.

The impact of information sharing on supply chains has become more significant with recent advances in Information Technology (IT). Furthermore, some investigations have been conducted to focus on the impact of information sharing on the product quality. However, there is still room for further studies to clarify exactly how and what information should be shared and the beneficial effects on quality improvement (Zahra Lotfi, Mukhtar, Sahran & Taei Zadeh, 2013).

There are many different types of information that can be shared within the supply chain, including logistics, business, strategic, tactical, etc. Some familiar types of Information may be categorized as Inventory Information, Sales Data, Sales Forecasting, Order Information, Product Ability Information, Exploitation Information of New Products, and other information.

In some cases, the information shared has to be strongly secured. Some classified documents, often in paper form, have to be shared in the supply chain management (Madenas, Tiwari, Turner & Woodward, 2014; Kobayashia, Tamakia & Komoda, 2003; Liua, Zhangb & Hu, 2005). These documents may be the subject of the RFID-based access control system.

The paper considers the problem of modeling and design of the RFID-based access control system. Subsequent chapters describe the system architecture and design models, including the domain model, requirements, business process models, and user interfaces.

2. SYSTEM ARCHITECTURE

A perspective of the module of privileges is shown in the following diagrams (Figure 1, Figure 2). The diagrams define the boundary of the module as well as the scope of data, which will be exchanged with external systems and databases.

The following diagram shows logical architecture of external interfaces of the system of the document lifecycle management. One of the system elements will be the module of privileges using some components of the workflow systems – Aurea BPM and Archer-DMS. All data concerning the privileges assigned to documents in Aurea BPM and Archer-DMS will be stored in separate Oracle databases.

The system will be compatible with other external systems, such as CrossTalk AppCenter and Cosmos. The integration will be made through appropriate program interfaces (Web service). The document flow management system will be also equipped with a graphical user interface (GUI) available from a web browser. The CrossTalkAppCenter and Cosmos systems also have user interfaces allowing their management and configuration.

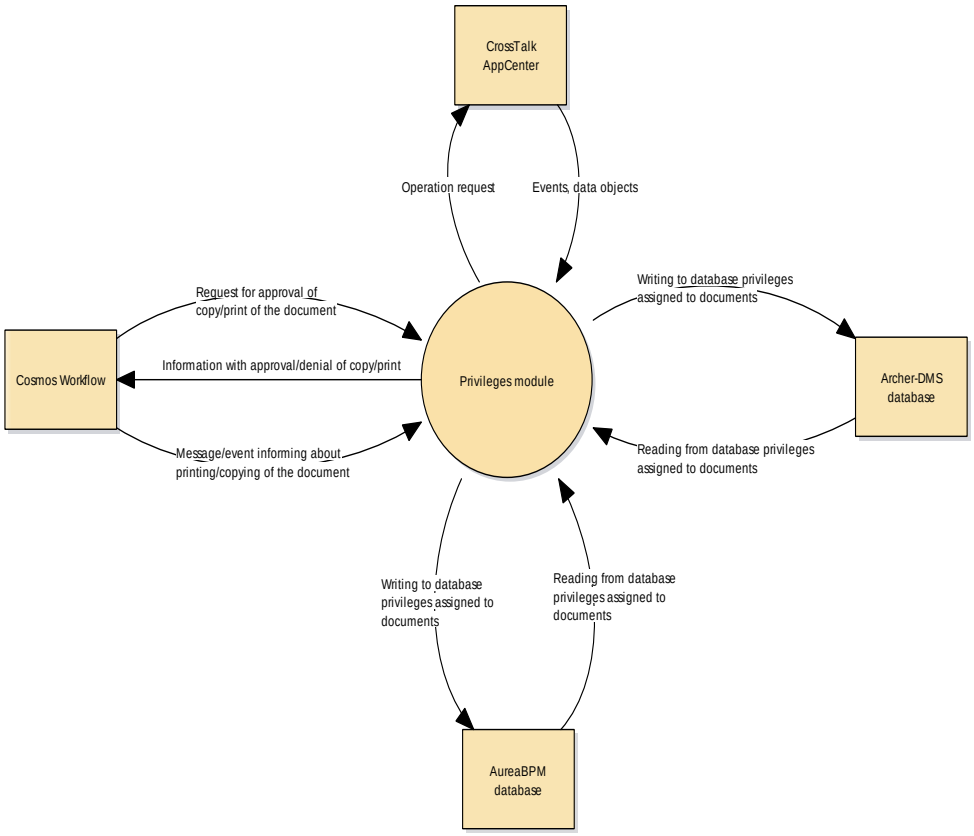

Fig. 1. Perspective of the module of privileges; own elaboration

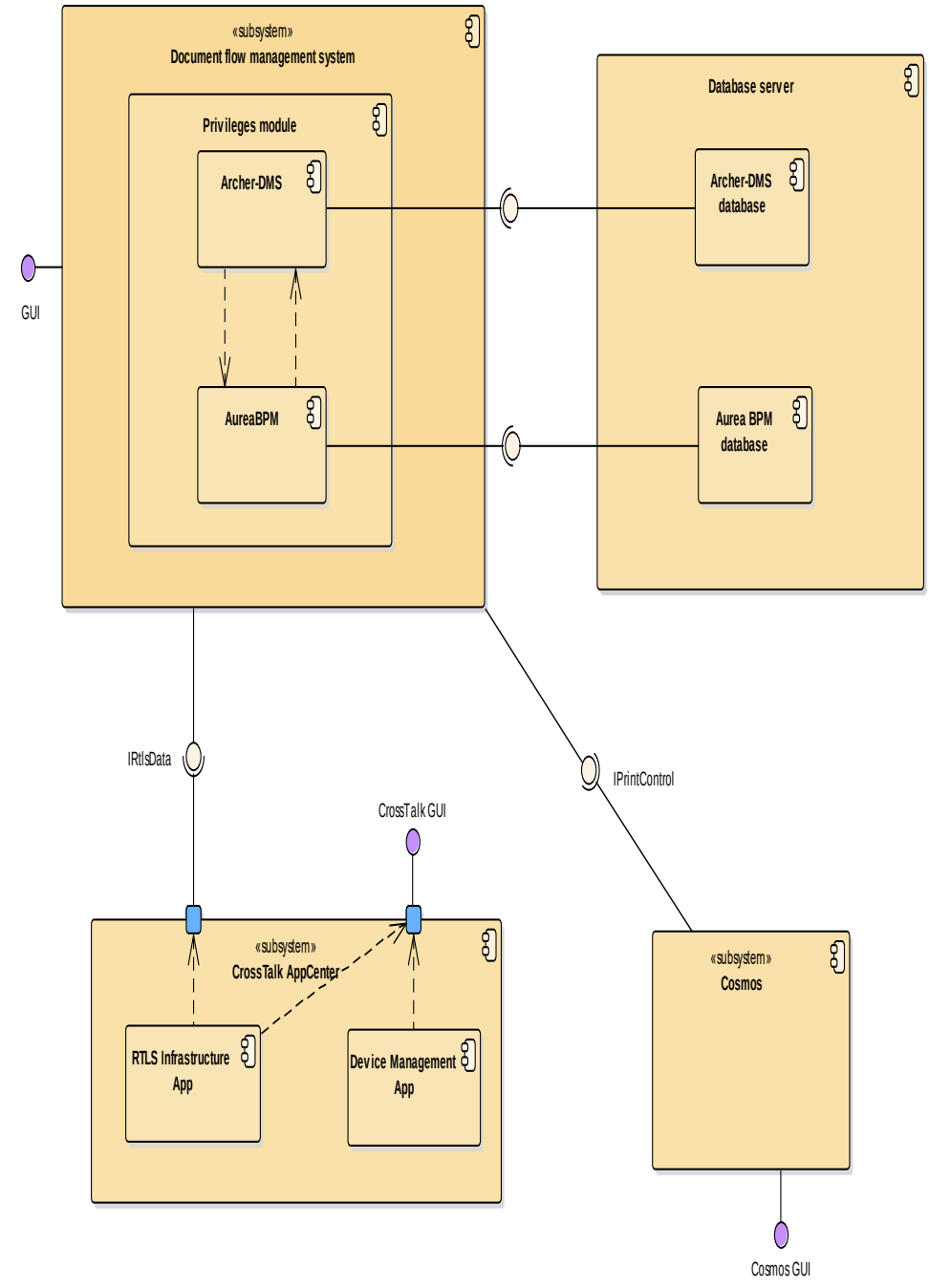

Fig. 2. Logical architecture of the privileges module; own elaboration

Table 1. Description of components of the logical architecture diagram

Element	Type	Description
Document flow management system	System	Electronic system for managing lifecycle of the documents at different sensitivity levels.
Privileges module	System module	Designed privileges module. Aurea BPM and Archer-DMS workflow systems will be used for the module.
Aurea BPM	System module	Workflow system allowing management and automation of business processes in the office.
Archer-DMS	System module	System responsible for the document management (paper and electronic).
Database server	Database server	Oracle database server
Aurea BPM database	Database	Database with user privileges to documents, assigned from the Aurea BPM system level
Archer-DMS database	Database	Database with user privileges to documents and privileges assigned to documents in Archer-DMS system
CrossTalkAppCenter	System	System for tracking the RFID-tagged objects
RTLS InfrastructureApp	System component	Component joining the RFID/RTLS physical devices with an application responsible for business logic The component captures location events from RFID/RTLS and sends the information on the location of the RFID-tagged objects to other systems.
Device Management App	System component	Administrative tool for configuration of the RFID/RTLS physical devices, configuration of messages exchanged between them and monitoring of the work of such devices.
Cosmos	System	System for managing the printing and copying of the documents by using the printing and copying office equipment.
IRtlsData	Interface	Web service interface for handling RTLS (Real-timelocating system) events generated by CrossTalkAppCenter on the basis of the information from the devices used for tracking the RFID-tagged objects The interface is responsible for integrating the document lifecycle management system with CrossTalkAppCenter in terms of handling RTLS (Real-timelocating system) events generated by CrossTalkAppCenter on the basis of the information from the devices used for tracking the RFID-tagged objects. The interface will allow to send the RTLS events.

IPrintControl	Interface	Web service interface for managing the printing and copying of the documents by using the printing and copying office equipment, including: verification of the user privileges to print or copy various documents, registration of events related to the printing and copying of the documents, registration and saving of the scanned documents (PDF files) in the database of the document lifecycle management system.
GUI	Interface	Graphical user interface of the document lifecycle management system used for the documents of different sensitivity levels, available from any web browser
CrossTalk GUI	Interface	Graphical user interface allowing configuration and administration of the infrastructure of the RFID/RTLS physical devices. The interface also allows the monitoring and visualization of the RFID-tagged tracking objects.
Cosmon GUI	Interface	Graphical user interface allowing the configuration of the workflow process for managing the printing and copying of the documents by using multifunction devices.

3. MAIN FEATURES OF THE ACCESS CONTROL SYSTEM

The main functions of the privileges module are the following:

1. document access control for persons with appropriate level and scope of privileges,
2. registration of new privileges assigned to users,
3. change of user privileges to handle the documents of different sensitivity levels,
4. storage of the information about the privilege level and scope for each document and each user,
5. management of privileges stored in the system,
6. registration of new users in the Aurea BPM and Archer-DMS systems,
7. control of the flow of media as well as classified and unclassified documents between different security zones, including the control of user privileges to classified and unclassified information,
8. protection of media and documents against unauthorized dislocation,
9. protection against multiple copying of the classified and unclassified documents,
10. control of the printing of the classified and unclassified documents with a limited number of copies,

11. identification of location of a single classified and unclassified document, with accuracy of the determined location of a folder or volume.

4. USERS OF THE ACCESS CONTROL SYSTEM

The privileges module was created to control access to records kept in the Secret Office by the employees. The employees of the Secret Office are the users of the system and hence the users of the privileges module. The role of an ordinary employee and administrator responsible for the system control in the Secret Office was distinguished. The system will be also compatible with other external systems, such as Cosmos and CrossTalk AppCenter.

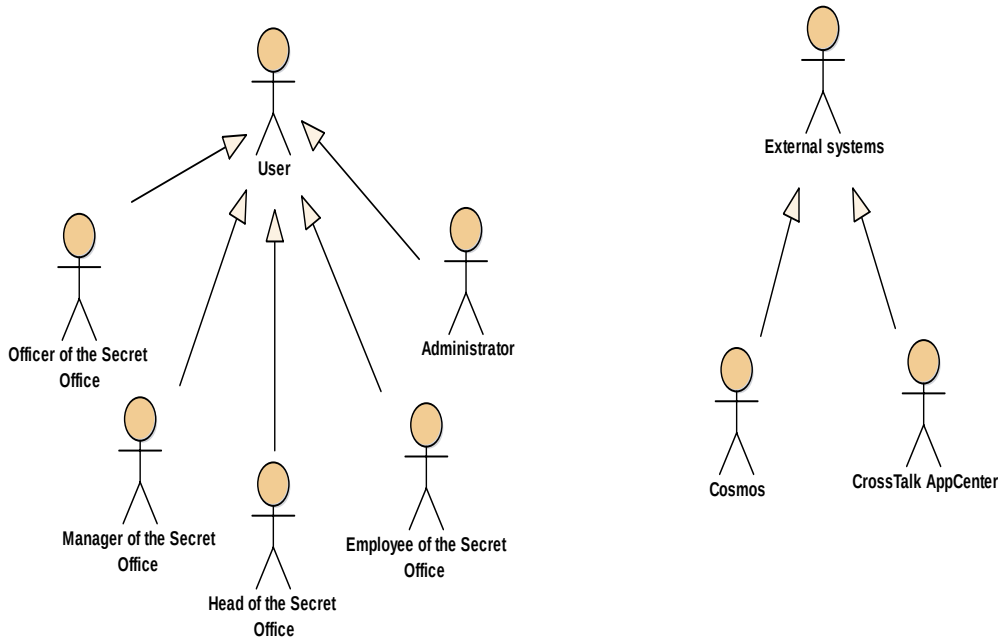

Fig. 3. System users; own elaboration

5. USE CASES

Basic functionalities to be provided by the document lifecycle management system are presented in the UML diagrams showing use cases (Waszkowski & Chodowska, 2012). Due to the size of such diagram, it was divided into two parts.

The first part describes use cases of the module of privileges in terms of handling the connection between CrossTalk AppCenter and Cosmos (Fig. 4).

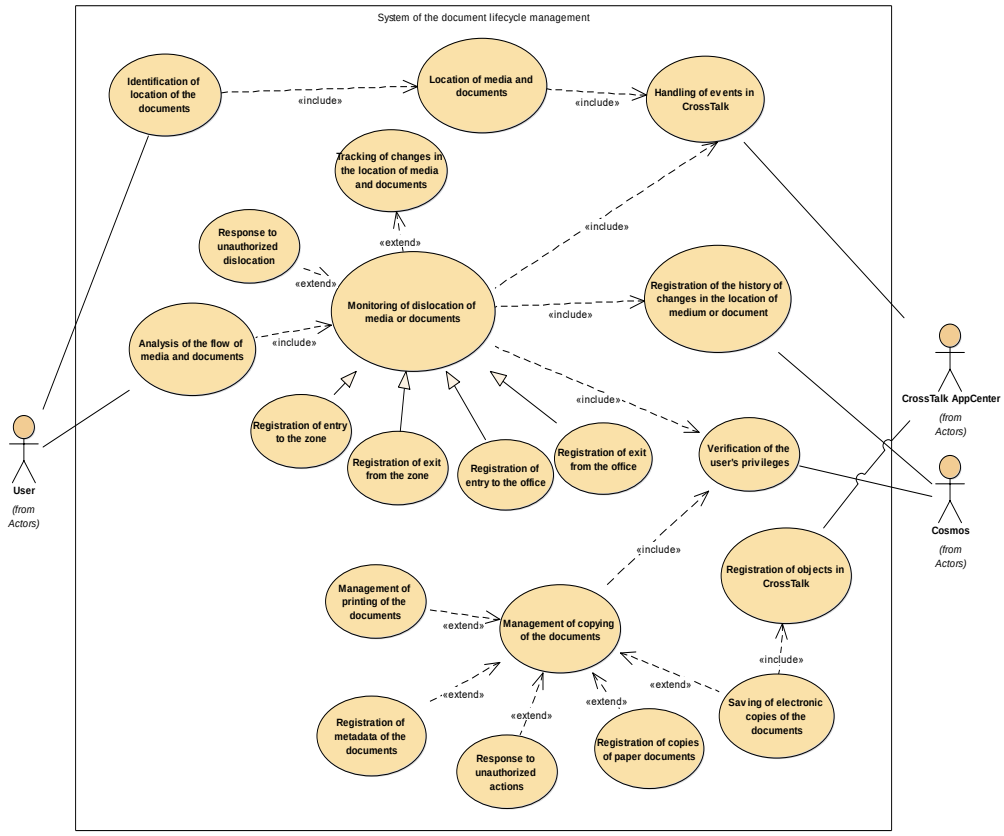

Fig. 4. Model of use cases; own elaboration

Table 2. Description of use cases – part 1

Use case	Description
Analysis of the flow of media and documents	The system allows analyzing the flow of media and documents within a single security zone as well as within different zones of the office.
Identification of location of the documents	The system enables the user to identify the location of the RFID-tagged media or documents within the area of the office. It is possible to locate the documents with accuracy of the location of the folder or volume.
Location of media and documents	The system allows to accurately locate the media or documents within the security zones in the office.

Monitoring of dislocation of media or documents	The system monitors and registers any changes of location of the media and documents within the office on an ongoing basis.
Handling of events in CrossTalk	The system allows to receive events from CrossTalk.
Response to unauthorized dislocation	The system will react to unauthorized dislocation of media or documents. The manner of the system's response will be determined at a later date (a model reaction of the system may be to send an appropriate alert message informing about a breach of security).
Registration of the history of changes in the location of medium or document	The system registers the history of changes in the location of media and documents, including the information on the users who downloaded them.
Registration of copies of paper documents	The system allows to register the copies of the RFID-tagged paper documents as subsequent copies.
Registration of metadata of the documents	The system allows to register metadata of the classified and unclassified documents.
Registration of objects in CrossTalk	The system ensures the sending of the information related to the registration of the new RFID-tagged object in the CrossTalk system.
Registration of entry to the office	The system registers entry of the document or medium to the RFID-tagged area of the office.
Registration of entry to the zone	The system registers entry of the document or medium to the RFID-tagged zone in the office.
Registration of exit from the office	The system registers exit of the document or medium from the RFID-tagged area of the office.
Registration of exit from the zone	The system registers exit of the document or medium from the RFID-tagged zone in the office.
Verification of the user's privileges	The system allows to verify the privileges of a given user to the document or types of the documents. The privileges will include, among other things, printing, copying, relocating documents within the zones of the office.
Saving of electronic copies of the documents	The system allows to save electronic copies of the documents from the copying devices in the office in the database.
Management of printing of the documents	The system allows to manage the printing of the classified and unclassified documents.
Management of copying of the documents	The system allows to manage the copying of the classified and unclassified documents.
Tracking of changes in the location of media and documents	The system automatically tracks and detects any changes in the location of the media and documents resulting from their relocation.
Response to unauthorized actions	The system will prevent any unauthorized actions of the users. A user's attempt to perform an action without authorization should be instantly banned and signaled in an appropriate message.

Another part of the diagram shows use cases developed with respect to the management of privileges assigned to users for the purpose of handling the documents as well as privileges and classification assigned to documents (Fig. 5).

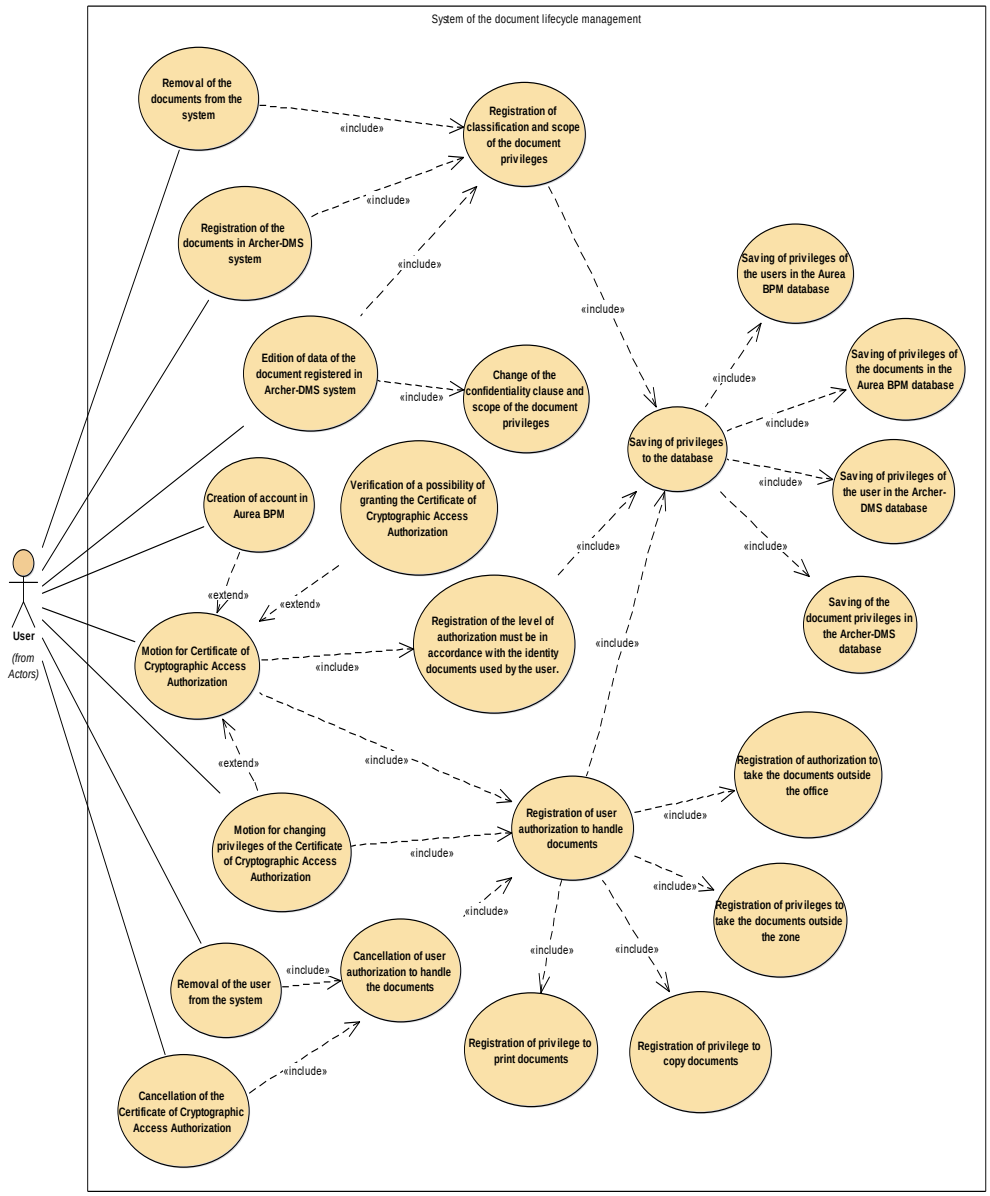

Fig. 5. Model of use cases; own elaboration

Table 3. Description of use cases – part 2

Use case	Description
Registration of the documents in Archer-DMS system	Each new document provided or created in the office will be registered in the Archer-DMS system. During registration, the documents are given appropriate classification and privileges.
Removal of the documents from the system	It is possible to remove the documents registered in Archer-DMS system. Removal of the document from the system will entail removal of all privileges assigned to this document.
Edition of data of the document registered in Archer-DMS system	The users will be able to edit data of each document registered in the Archer-DMS system provided that they have been authorized to do so.
Change of the confidentiality clause and scope of the document privileges	The authorized users will be able to change classification of the document and privileges to handle it.
Registration of classification and scope of the document privileges	All changes related to the documents will be registered in Archer-DMS and Aurea BPM systems. The above-mentioned changes include: entry of a new document into the system, edition of the document, removal of the document. Each change will affect the privileges and classification of the documents.
Saving of privileges to the database	All changes in the privileges and classification of the documents as well as privileges of the users will be saved in the Oracle database. The privileges should be saved in both databases of the Aurea BPM and Archer-DMS systems.
Saving of privileges of the users in the Aurea BPM database	All changes in the user privileges should be saved in the Aurea BPM database.
Saving of privileges of the documents in the Aurea BPM database	All changes in the document privileges should be saved in the Aurea BPM database.
Saving of privileges of the user in the Archer-DMS database	All changes in the user privileges should be saved in the Archer-DMS database.
Saving of the document privileges in the Archer-DMS database	All changes in the document privileges should be saved in the Archer-DMS database.
Motion for Certificate of Cryptographic Access Authorization	To obtain authorization to handle the documents, the user should file a motion in the Aurea BPM system. In the motion, the user should specify to which document it wants to have access authorization and what kind of privileges it actually needs. The user will obtain privileges once the motion has been considered favorably.
Creation of account in Aurea BPM	When filing the motion for access authorization to documents, the employee should have an account in the Aurea BPM

	system. If the employee does not have such account, it may file the motion from a temporary account after being assigned an appropriate token. In such case, the employee includes in the motion a need for creating the aforementioned account. The information about the need to create the account should be sent to the System Administrator in the Secret Office. The Administrator will create such account and further steps of the process related to the submission of the motion will be undertaken by the user from his/her account.
Motion for changing privileges of the Certificate of Cryptographic Access Authorization	The user who is already authorized will be able to file a motion for changing his/her privileges. The change of privileges will be effectuated once the motion has been considered favorably.
Verification of a possibility of granting the Certificate of Cryptographic Access Authorization	Duly authorized users responsible for considering the motions for the Certificates of Cryptographic Access will be able to verify whether the granting of privileges to handle the documents is justified.
Registration of the level of authorization must be in accordance with the identity documents used by the user.	All privileges assigned to the user should be in compliance with the identity documents used by the users. The documents are issued by appropriate bodies.
Registration of user authorization to handle documents	Favorable consideration of the motion for the Certificate of Cryptographic Access Authorization or change of authorization will result in the registration of new privileges to handle the documents.
Registration of authorization to take the documents outside the office	The authorization to take the document outside the designated area of the office will be registered. Taking the documents outside the office will be possible only in case of the users who have cards with the RFID chip, where the user IDs are recorded. The use of the card on an appropriate reader should allow to read from the authorization system.
Registration of privileges to take the documents outside the zone	The authorization to the document outside the designated zone will be registered. Taking the documents outside the designated zone will be possible only in case of the users who have cards with the RFID chip, where the user ID is recorded. The use of the card on an appropriate reader should allow read from the authorization system.
Registration of privilege to copy documents	The authorization to copy the documents will be registered. The documents may be copied only by the users who have cards with the RFID chip, where the user ID is recorded. The use of the card on an appropriate reader should allow read from the authorization system. The RFID readers will be mounted on photocopiers.

Registration of privilege to print documents	The authorization to print the documents will be registered. The documents in electronic form may be printed only by the users who have cards with the RFID chip, where the user ID is recorded. The use of the card on an appropriate reader should allow read from the authorization system. The RFID readers will be mounted on printers.
Removal of the user from the system	Each registered user may be removed from the system. The removal of the user from the system will result in the removal of his/her authorization to handle the documents.
Cancellation of the Certificate of Cryptographic Access Authorization	The user may file an appropriate motion to cancel the Certificate of Cryptographic Access Authorization . It will change the user's privileges.
Cancellation of user authorization to handle the documents	Removal of the Certificate of Cryptographic Access Authorization or user's account causes the removal of the user's privileges.

6. CONCLUSION

This paper outlines the concept and design models of the access control system for the RFID-tagged documents in the supply chain management. The research was performed as part of the second R&D project no. DOBR-BIO4/006/13143/2013.

As part of the implementation of this project, the module of privileges including the user authorization to handle the documents at different sensitivity levels was developed. The level of privileges should be confirmed by appropriate certificates issued by relevant authorities. The designed module of privileges will use the functionalities of the Aurea BPM and Archer-DMS systems. Within the framework of the privileges module, the information on the level and scope of privileges to each document and each person handling the documents is stored in the system.

As part of further research, to facilitate proper functioning of the privileges module, the document flow processes in terms of receiving and accepting motions for granting privileges will be designed and implemented.

ACKNOWLEDGEMENTS

This work was created as part of the project DOBR-BIO4/006/13143/2013 supported by NCR&D.

REFERENCES

Kee-hung Lai, Wong Ch.W.Y. & Siu Lee Lam J. (2015), Saring environmental management information with supply chain partners and the performance contingencies on environmental munificence, Int. J. Production Economics 164, pp. 445–453.

Kobayashia T., Tamakia M. & Komoda N. (2003), Business process integration as a solution to the implementation of supply chain management systems, Information & Management Vol. 40, pp. 769–780.

Liua J., Zhangb S. & Hu J. (2005), A case study of an inter-enterprise workflow-supported supply chain management system, Information & Management, Vol. 42, pp. 441–454.

Madenas N., Tiwari A., Turner Ch.J. & Woodward J. (2014), CIRP Journal of Manufacturing Science and Technology, Vol. 7,pp. 335–346.

Waszkowski R. & Chodowska A. (2012), Modele procesów z wykorzystaniem ścieżek alternatywnych wykorzystywanych w zależności od rezultatów działania podsystemów wspomagania decyzji opartych na modelach dynamicznych oraz symulacji komputerowej, Modelowanie i symulacja procesów oraz określenie komputerowo wspomaganych procedur w zakresie zarządzania ryzykiem bezpieczeństwa żywności i żywienia, J. Bertrandt, K. Lasocki (ed.), Warsaw, BEL Studio, pp. 890-919.

Zahra Lotfi, Mukhtar M., Sahran S. & Taei Zadeh A. (2013), Information Sharing in Supply Chain Management, Procedia Technology 11, pp. 298–304.