Business processes in the RFID-equipped restricted access administrative office

Waszkowski Robert[1,a], Kiedrowicz Maciej[1], Nowicki Tadeusz[1], Wesołowski Zbigniew[1] and Worwa Kazimierz[1]

[1]Military Academy of Technology, Faculty of Cybernetics, Kaliskiego 2, 00-908 Warsaw, Poland

Abstract. The paper presents business processes in the RFID-equipped restricted access administrative office. The presented diagrams are the result of the analytical work performed by the multidisciplinary team of experts. The team was composed of IT specialist, security systems specialists and employees of the secret office. The presented models include the fact that the facilities in the secret office (cabinet, sluice, photocopier, desks) are equipped with the RFID reader, which allows to immediately read the documents that are within their reach.

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 for Polish enterprises.

However, paper documents still remain of great importance. Agreements, certificates, securities, deeds, records of employees are some of the examples of the documents stored in paper form.

Both storage and archiving of such documents as well as access management constitute a challenge and very often require the use of certain IT-supported procedures.

The 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 the RFID tags makes it possible to obtain an automated document management system. It offers great opportunities in the field of document security, accountability and traceability.

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

The basic functionalities of the system include:

- remote identification of unclassified and classified data storage devices labelled for real-time radio-reading at the storage and work location;
- automatic inventory of unclassified and classified documents arranged in piles and filed, including automatic detection of relocation;
- control of the movement of data storage devices as well as unclassified and classified documents across security zones, including access control of unclassified and classified documents;
- protection of data storage devices and documents against unauthorized relocation;
- automatic identification of data storage devices and documents not only at the storage location, but also at workstations;
- protection against repeated copying of unclassified and classified documents;
- control of printing of unclassified and classified documents with a copy limit;
- identification of the location of individual unclassified and classified documents with a pre-set accuracy of a file or volume location.

The document lifecycle management, built on the basis of the Business Process Management System, is used by the personnel of the restricted access to an administrative office, where the system is to be implemented. The system co-operates with the following external systems: CrossTalkAppCenter and Cosmos. It is integrated via adequate programming interfaces (Web service). The document flow management system also has a graphic user interface (GUI) accessible from the Internet browser level. CrossTalkAppCenter and Cosmos also have user interfaces enabling their control and configuration (Figure 1.).

[a] Corresponding author: robert.waszkowski@wat.edu.pl

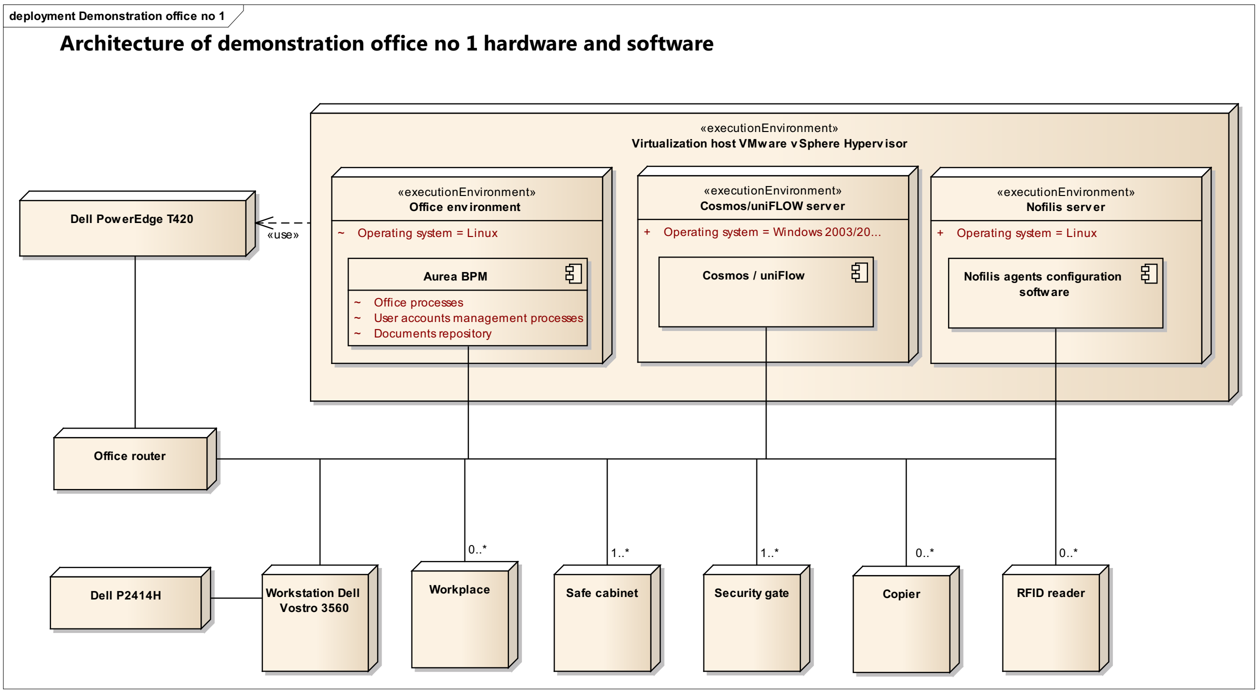
deployment Demonstration office no 1
Architecture of demonstration office no 1 hardware and software
«executionEnvironment»
Virtualization host VMware vSphere Hypervisor
«executionEnvironment»
Office environment
~ Operating system = Linux
Aurea BPM
~ Office processes
~ User accounts management processes
~ Documents repository
«executionEnvironment»
Cosmos/uniFLOW server
+ Operating system = Windows 2003/20...
Cosmos / uniFlow
«executionEnvironment»
Nofilis server
+ Operating system = Linux
Nofilis agents configuration software
Dell PowerEdge T420
«use»
Office router
Dell P2414H
Workstation Dell Vostro 3560
Workplace
Safe cabinet
Security gate
Copier
RFID reader
0..*
1..*
1..*
0..*
0..*

Figure 1. Architecture of the classified document lifecycle management system

2 Business processes of the RFID-equipped restricted access administrative office

As a result of the analytical work, the following business processes of the secret office equipped with the RFID devices have been defined:
- acceptance of the document or documents with the RFID tags from a natural person,
- acceptance of a parcel with documents including the RFID tags, with traces of opening,
- performance of standard procedures when receiving the RFID tagged documents,
- registration of correspondence in the form of the RFID tagged documents,
- classification of the RFID tagged documents,
- registration of the created RFID tagged documents,
- processes related to the storage of the RFID tagged documents,
- preparation for dispatch of the RFID tagged documents,
- sending of the RFID tagged documents via a carrier,
- making the RFID tagged documents available,
- destruction of the RFID tagged documents.
The subsequent chapters outline the most important of these processes.

3 Parcel receipt business process

The parcel receipt business process (Figure 1) is implemented according to the following scenario:

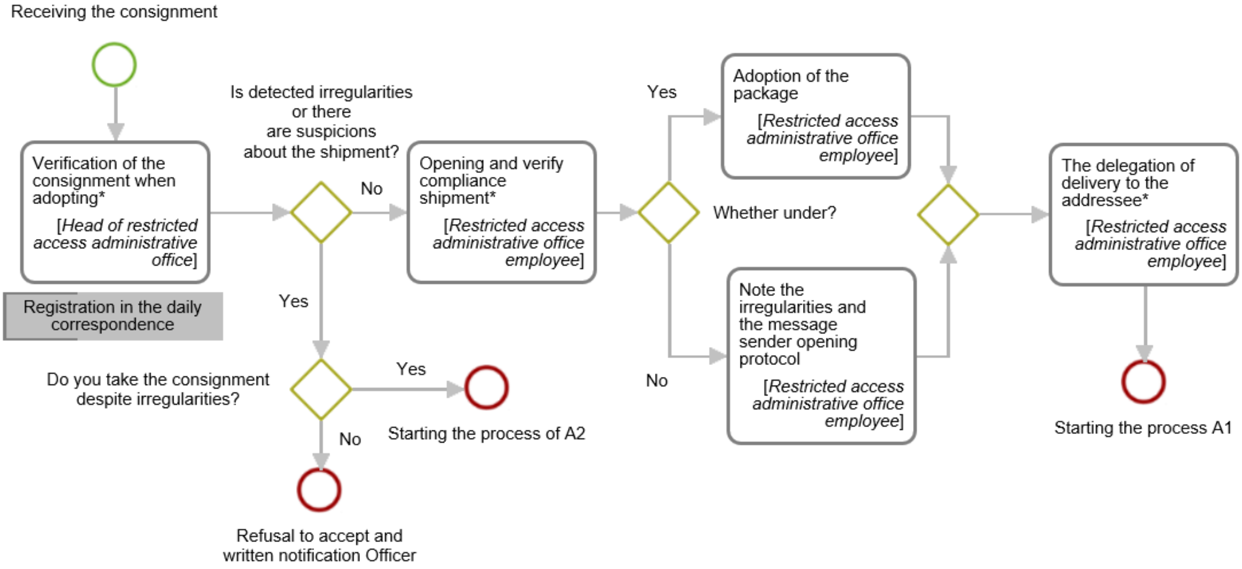
Receiving the consignment
Verification of the consignment when adopting*
[Head of restricted access administrative office]
Registration in the daily correspondence
Is detected irregularities or there are suspicions about the shipment?
No
Yes
Opening and verify compliance shipment*
[Restricted access administrative office employee]
Do you take the consignment despite irregularities?
Yes
No
Starting the process of A2
Refusal to accept and written notification Officer
Yes
No
Whether under?
Adoption of the package
[Restricted access administrative office employee]
Note the irregularities and the message sender opening protocol
[Restricted access administrative office employee]
The delegation of delivery to the addressee*
[Restricted access administrative office employee]
Starting the process A1

Figure 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), who prepares a start-up form on the date of acceptance of the consignment, enters the data into the records of delivery / schedule of shipments and approves the task.
2. Then the Director receives the consignments and checks them on entry. (S)he introduces the data upon receipt, whereas the sender acknowledges safe receipt of the shipment and enters the data to verify 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 or not, despite certain irregularities:
   a. If not, (s)he refuses to accept the shipment and does not notify the authority in writing. This ends the process.
   b. If yes, (s)he starts the process of "acceptance of the damaged or opened parcel".
5. The secret office manager hands over the parcel to an employee of the secret office.
6. The employee opens the parcel.
7. The secret office employee checks the compatibility between the contents of the consignment and the locator numbers inside the envelope.
8. The secret office employee verifies the number of pages, attachments and pages of appendices according to the numbers indicated on the individual cryptographic media.
   a. If the employee finds any irregularities, (s)he makes an entry into the parcel opening register, describing the existing irregularities and includes this information in the official correspondence. Subsequently, (s)he attaches the opening confirmation letter to the cryptographic materials. Then (s)he sends the opening confirmation letter to the original parcel sender (go to step 10).
9. The secret office employee accepts the parcel.
10. The secret office employee forwards the parcel in the following manner:
   a. If it is an urgent parcel, go to step 11.
   b. If it is an ordinary parcel, an office worker may be in no hurry with the transfer of the consignment. The employee stars the process of the "registration of the document in the restricted access administrative office".
11. The secret office employee passes the parcel immediately. (S)he includes this fact in the notes of the muster apparatus specifying the date and time of the delivery. The employee starts the process of the "registration of the document in the restricted access administrative office".

4 Business process registration of the document in the restricted access administrative office

The business process - "Registration of the document in the restricted access administrative office" (Figure 2) is implemented according to the following scenario:

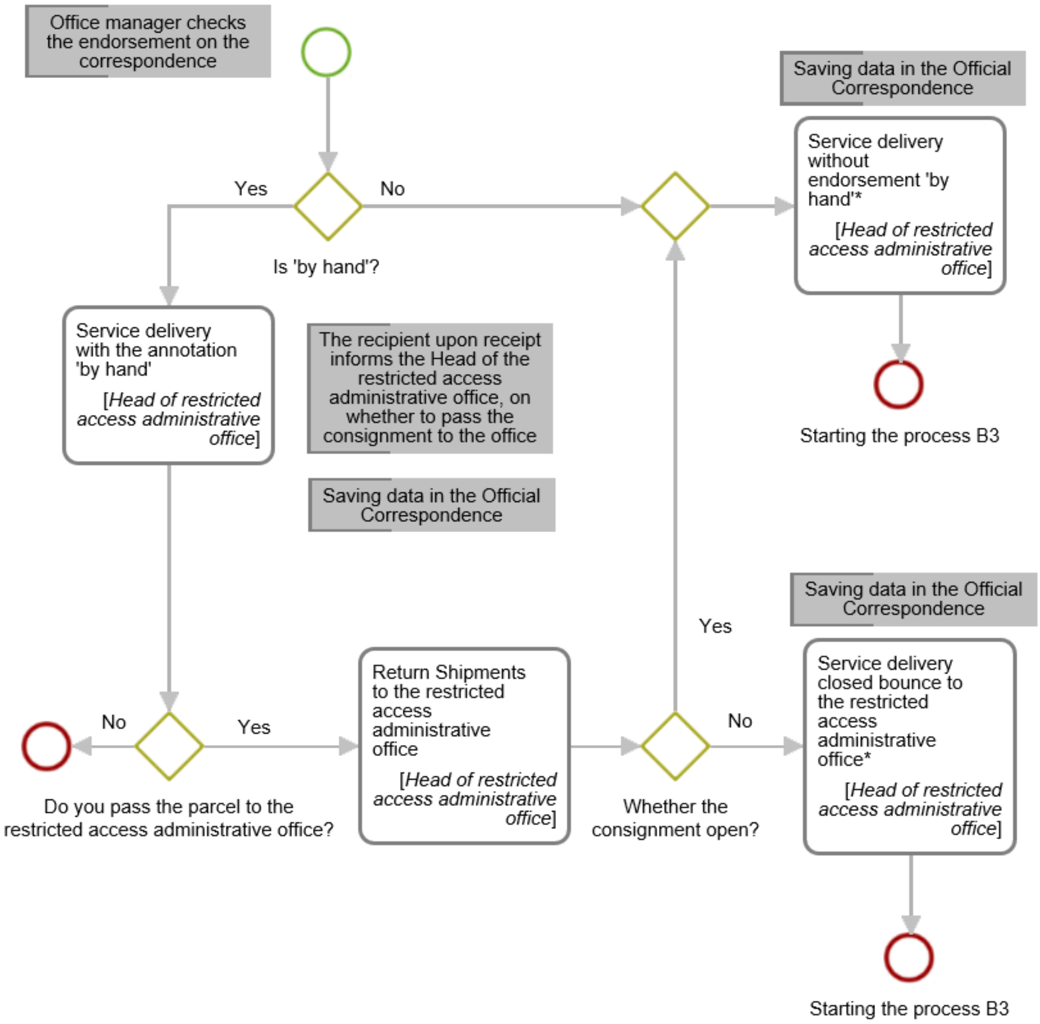
Office manager checks the endorsement on the correspondence
Yes
No
Is 'by hand'?
Saving data in the Official Correspondence
Service delivery without endorsement 'by hand'*
[*Head of restricted access administrative office*]
Starting the process B3
Service delivery with the annotation 'by hand'
[*Head of restricted access administrative office*]
The recipient upon receipt informs the Head of the restricted access administrative office, on whether to pass the consignment to the office
Saving data in the Official Correspondence
Yes
Saving data in the Official Correspondence
No
Yes
Do you pass the parcel to the restricted access administrative office?
Return Shipments to the restricted access administrative office
[*Head of restricted access administrative office*]
No
Whether the consignment open?
Service delivery closed bounce to the restricted access administrative office*
[*Head of restricted access administrative office*]
Starting the process B3

Figure 3. Registration of the document in the restricted access administrative office (source: own elaboration).

1. The head of the secret office or other authorized employee verifies whether the correspondence contains the notation 'by hand':
   a. If not, go to 2.
   b. If yes, go to 7.
2. The head of the secret office or other authorized employee applies a stamp effect on the first page of the cryptographic material.
3. The head of the secret office or other authorized employee makes seal imprints on the annexes.
4. The head of the secret office or other authorized employee completes more items in the official correspondence.
5. The head of the secret office or other authorized employee enters the date of registration in the document.
6. The head of the secret office or other authorized employee enters the item the "document storage" is initiated.
7. The head of the secret office or other authorized employee leaves the shipment in a closed inner wrapping.
8. The head of the secret office or other authorized employee includes in the official correspondence the information contained in the inner packaging.
9. The head of the secret office or other authorized employee includes in the official correspondence date of receipt.
10. The head of the secret office or other authorized employee puts the notation 'by hand' in the Comments section.
11. The head of the secret office or other authorized employee puts the stamp imprints on the consignment.
12. The head of the secret office or other authorized employee includes a registration number in the official correspondence.
13. The head of the secret office or other authorized employee puts the date information on the consignment.
14. The head secret office or other authorized employee transfers the load directly to the addressee or authorized person.
15. The recipient or authorized person decides whether the consignment will be sent back to the office:
   a. If yes, go to 16.
   b. If not, end the process.

16. The recipient or person authorized returns the parcel to the office:
    a. Parcel opened (go to 2).
    b. Parcel closed (go to 17).
17. If the service delivery is closed the shipment is returned to the office. The head of the secret office or other authorized employee puts the stamp imprints in the form of round numbers or their names.
18. The head of the secret office or other authorized employee notes that the consignment is stored in the form of a sealed package in the "Remarks" section in the official correspondence. The process of the "document storage" is initiated.

5 Business process “Security classification granting”

The business process - “Security classification granting” (Figure 3) is implemented according to the following scenario:

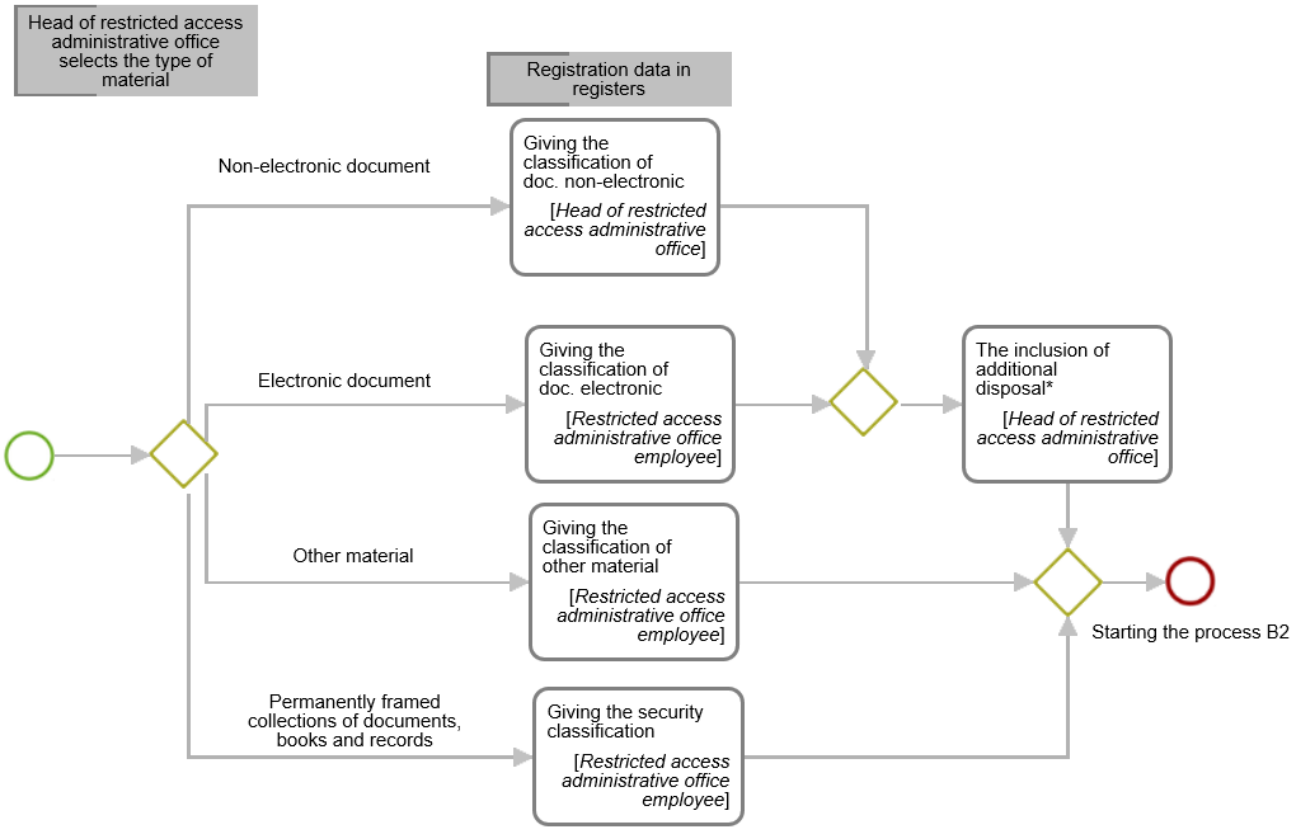
Head of restricted access administrative office selects the type of material
Registration data in registers
Non-electronic document
Giving the classification of doc. non-electronic [Head of restricted access administrative office]
Electronic document
Giving the classification of doc. electronic [Restricted access administrative office employee]
The inclusion of additional disposal* [Head of restricted access administrative office]
Other material
Giving the classification of other material [Restricted access administrative office employee]
Starting the process B2
Permanently framed collections of documents, books and records
Giving the security classification [Restricted access administrative office employee]

Figure 4. Security classification granting (source: own elaboration).

1. The person responsible for assigning clauses on the start-up form selects the type of material and approves the task:
    a. If a non-electronic document is selected, the task “Classifying the doc. as non-electronic” is started. The head of the restricted access administration office enters the following data:
        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 “Classifying the doc. as electronic” is started (go to 15).
    c. If other materials are selected, the task “Classifying other material” is started (go to 24).
    d. If a tightly sealed set of documents, books and records are selected, the task “Security classification” is started (go to 25).
2. The responsible person puts the security classification at the centre, as the first element in the header and footer.
3. The responsible person types the copy number, or, in case of a single copy, enters "Single".
4. The responsible person affixes a digital signature.
5. The responsible person enters page numbers and the number of pages in the entire document.
6. The responsible person adds additional instructions.
7. The responsible person enters the name of the entity or organizational unit.
8. The responsible person enters the name of the place and date of signing the document.
9. In the case of a document that has been provided in the course of the correspondence, the responsible person enters his/her name or the name of the recipient.
10. The responsible person enters the number of attachments and number of pages.

11. The responsible person enters the security classification attachments with the numbers under which they were registered.
12. The responsible person enters the position and name of the person authorized to sign the documents.
13. The responsible person enters the number of copies made and recipients of individual copies.
14. The responsible person enters the name of the contractor. Then, (s)he adds the supplementary information and starts the process of the "registration of the produced materials".
15. The responsible person enters the security classifications in the metrics form.
16. The responsible person affixes a digital signature.
17. The responsible person enters the name of the entity or organizational unit.
18. The responsible person enters the document's registration date.
19. In the case of a document that has been provided in the course of the correspondence, the responsible person enters his/her name or the name of the recipient.
20. The responsible person enters the security classification attachments with the numbers under which they were registered.
21. The responsible person enters the position and name of the person authorized to sign the documents.
22. The responsible person enters his/her name and the name given to the document or the signature of the author.
23. The responsible person enters the name given to the document or determines which document is discussed. The responsible person enters the supplementary information and then starts the process of the "registration of the on-site prepared materials".
24. The responsible person enters the classification and affixes the digital alphanumeric signature by way of stamping/printing/permanent marking on the casing or packaging. The process of the "registration of the on-site prepared materials" starts.
25. The responsible person enters the classification clause on the outer walls of the cover and the title page. The process of the "registration of the on-site prepared materials".

6 Business process "Shredding of cryptographic documents"

The business process – "Shredding of cryptographic documents" (Figure 4) is implemented according to the following scenario:

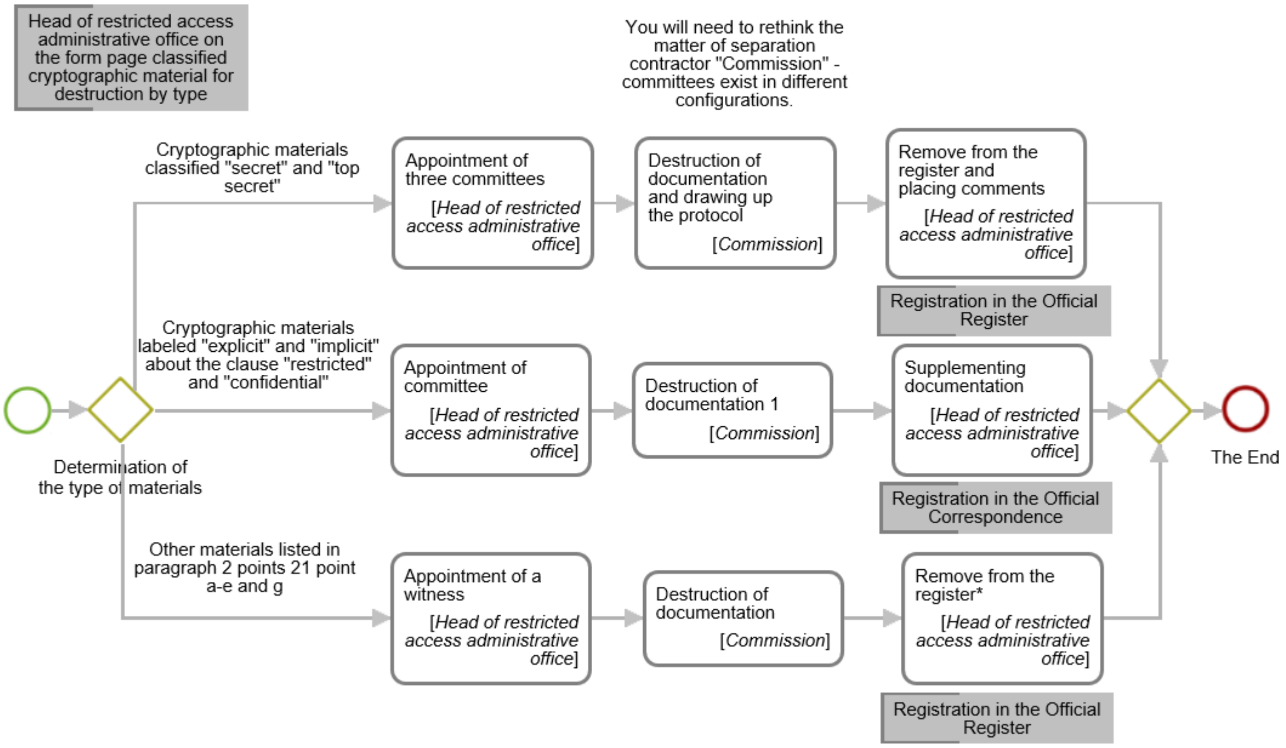
Head of restricted access administrative office on the form page classified cryptographic material for destruction by type
You will need to rethink the matter of separation contractor "Commission" - committees exist in different configurations.
Cryptographic materials classified "secret" and "top secret"
Appointment of three committees [Head of restricted access administrative office]
Destruction of documentation and drawing up the protocol [Commission]
Remove from the register and placing comments [Head of restricted access administrative office]
Registration in the Official Register
Cryptographic materials labeled "explicit" and "implicit" about the clause "restricted" and "confidential"
Appointment of committee [Head of restricted access administrative office]
Destruction of documentation 1 [Commission]
Supplementing documentation [Head of restricted access administrative office]
Registration in the Official Correspondence
Determination of the type of materials
The End
Other materials listed in paragraph 2 points 21 point a-e and g
Appointment of a witness [Head of restricted access administrative office]
Destruction of documentation [Commission]
Remove from the register* [Head of restricted access administrative office]
Registration in the Official Register

Figure 5. Shredding of cryptographic documents (source: own elaboration)

1. On the start-up form, the head of the secret office classifies the materials to be destroyed by their type (the documents stored in the computer databases are not to be destroyed):
    a. If the cryptographic material is classified as SECRET and TOP SECRET, the task Appointment of three commission members (go to step 2) is initiated.
    b. If the cryptographic materials designated as EXPLICIT and CLASSIFIED, the task to set up the commission (go to step 6) is initiated.

   c. Other materials: cryptographic system components (block module, component and auxiliary cryptographic devices), cryptographic products, publications and cryptographic technical documentation, cryptographic systems and products, forms and other registration devices to start the task aimed at calling a witness (go to 10).

2. The head of the organizational unit is appointed and at least 3 persons from the commission.
3. The commission shreds the documentation.
4. The commission draws up the minutes.
5. The manager of the organization removes documentation from the register and the information about this event is included therein. The process ends.
6. The manager of the organization appoints a committee composed of the office staff or contractor.
7. The commission shreds the documentation.
8. The manager of the organization enters in the "Remarks" muster apparatus annotation that reads: "destroyed by …".
9. The manager of the organization completes the date and ensures that the legible signatures of the persons involved in the destruction of the cryptographic materials are affixed. The process ends.
10. The manager of the organization appoints a witness: Deputy Chief Registry Officer or any other person holding a security clearance.
11. The commission destroys the documentation.
12. The manager of the organization confirms the destruction on the form AF 21 PL.
13. The manager of the organization removes documentation from the register and the information about this event is included therein. The process ends.

7 Conclusion

The management of the classified and non-classified document flow, the document access control, supervision of their copying as well as the document access management constitute basic functions of the solution proposed in the research project,

The results of the project will be used in the document management systems, local organizations, banks, government organizations. These systems store personal data or corporate data as well as support document flow between different organizations.

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

Both the increasing of the security level of the documents as well as the authorized persons will improve the quality of the entire process associated with the document flow. The most tangible result of these actions will be the reduction (eventually - total liquidation) of incidents related to the uncontrolled disclosure of the classified documents and data. It is of great importance from the point of view of state safety, which nowadays may be even related to terrorist threats. Poland, as a member of the European Union and NATO, is obliged to exert certain efforts to protect the processing of sensitive information.

An additional advantage of the proposed solutions, apart from providing better control over the storage and document sharing, will be a possibility of tracing the document flow between safety zones, with knowledge of the authorized persons that have been using the documentation. Mapping of the flow of the classified documents, in case of an incident, will allow effective investigation of the causes of their occurrence and making a list of the persons potentially responsible thereof.

The main users of the system will be units of state administration, including institutions subordinate to the Ministry of National Defence and the Ministry of the Interior and Administration. An important field of application of 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, and 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 - the police, prosecutors, ordinary and administrative, regional, district and appellate courts use documents in paper form. In accordance with the Polish and European legislation, most of the paper documents constitute evidence in the police investigation, prosecution and court proceedings, and, consequently, it is impossible to convert them into an electronic form – they have to remain in their traditional paper form.

Another example are various medical records produced by different institutions participating in the healing process. Taking into account the size of the produced medical records, their current storage and backup, clinics and hospitals are faced with a serious challenge. Therefore, the use of the results of the project would provide huge benefits for this industry 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 information on the historical society, history of the Polish nation and our statehood. The purpose of the state archives today is also to secure archival materials created in the public sector. The application of the project to check archival resources already at its creation in the institutions that have archival materials, will allow to secure historical resources through supervision and control of the movements of the labelled media. Miles and miles of archives collected in different archives (for example, 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 the documents to be more effectively protected against any damage or theft both during their storage and access.

The system, based on the RFID technology, may also be applied to other institutions, which store archival materials, such as libraries, museums and documentation centres, etc. The library may 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 the advanced solutions based on the radio and automatic document identification does not exist in Europe. With such technology, Polish institutions and companies become a leading supplier of the solutions for the European market, and later also worldwide.

Acknowledgements

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

References

1. Finkenzeller K., RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition, John Wiley & Sons (2003)
2. Cole P.H., Ranasinghe D.C., Networked RFID Systems and Lightweight Cryptography, Springer (2008)
3. Zhang Y., Yang L.T., Chen J., RFID and Sensor Networks Architectures, Protocols, Security and Integrations, CRC Press (2009)
4. Paret D., RFID at Ultra and Super High Frequencies. Theory and application, John Wiley & Sons (2009)
5. Bolic M., Simplot-Ryl D., Stojmenovic I., RFID Systems Research Trends And Challenges, John Wiley & Sons (2010)
6. Miles S.B., Sarma S.E., Williams J.R., RFID Technology and Applications, Cambridge University Press (2008)
7. noFilis “CrossTalk AppCenter 3.0 Installation and Administration Guide”
8. Canon UniFLOW documentation - www.canon.com
9. Aurea BPM system documentation - aurea-bpm.com
10. Braude E.J., Bernstein, M.E., Software engineering: modern approaches, J. Wiley & Sons (2011)
11. Larman, C., Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development, 3/e, Pearson Education India (2012)
12. http://aurea-bpm.com