Integrating RFID and Security Devices for an Innovative System to Manage Classified Documents

Elena Stringa, Claudio Bergonzi and Graziano Azzalin

European Commission – Joint Research Centre, Via Fermi 2749, 21027 Ispra, Italy

Abstract. This paper presents an innovative RFID solution to manage sensitive document archives. The system aims at: i) automatically tracing all document accesses at level of each page (who read the document and when); ii) knowing at any time where a document is; iii) providing periodical archive inventory; and iv) automatically signaling anomalies detected in the archive. The system represents an important tool for national/international security, as it allows a quick document recovery in case of emergencies. Moreover, with the proposed system the institution in charge of sensitive document archives can demonstrate the secure management of the entrusted material. This paper describes how the system has been implemented and reports tests performed in laboratory by simulating different scenarios, showing that the solution allows a reliable management of sensitive documents.

1 Introduction and State of the Art

According to European Commission decision 2001/844, classified documents are marked "RESTRICTED", "CONFIDENTIAL", "SECRET" or "TOP SECRET" depending on the impact that their content diffusion may have on the security of the European Union or of its Member States. Sensitive documents should be treated according to the following requirements:

- the original document and all its authorized copies should be authenticated,
- all the documents should be archived in a restricted and controlled access area,
- only authorized persons can consult the documents and the document access should be registered,
- the inventory of the archive should be performed periodically.

Currently, all the operations to manage classified documentation are carried out by operators with the only support of database technology for document archive organization. Database updating, archive inventory, document authentication and integrity verification are carried out manually; therefore, there is the need to develop a system to support the security archive responsible in the document management tasks.

On the market, Radio Frequency Identification (RFID)-based systems for library management can be found [1], [2], [3]. They are based on high frequency (HF) low cost tags, allowing theft prevention and more efficient tracking and inventory of

Stringa E., Bergonzi C. and Azzalin G.
Integrating RFID and Security Devices for an Innovative System to Manage Classified Documents.
DOI: 10.5220/0003007300890096
In *Proceedings of the 4th International Workshop on RFID Technology - Concepts, Applications, Challenges (ICEIS 2010)*, page
ISBN: 978-989-8425-11-9

items [4]. Unfortunately, available systems do not verify document authentication and integrity, e.g. the replacement of a document page with another one. On the market it is possible also to find high frequency (HF) RFID tags (Magellan PJM Stack tags ®) that can be overlapped without generating mutual interference problems. These tags would allow document tracing at level of single pages, but so far such application does not exist. Moreover, a solution similar to the one we are presenting in this paper, integrating security features to document management, satisfying the previously mentioned requirements is not yet present in the state of the art.

2 The Implemented System

Fig. 1 shows the scheme of the setup document archive. The archive mock-up consists of three bookshelves, each of them composed of four cells. The shelf doors are equipped with magnetic contacts, controlled by an input/output device (Adam 6060W from Advantech) to detect door opening.

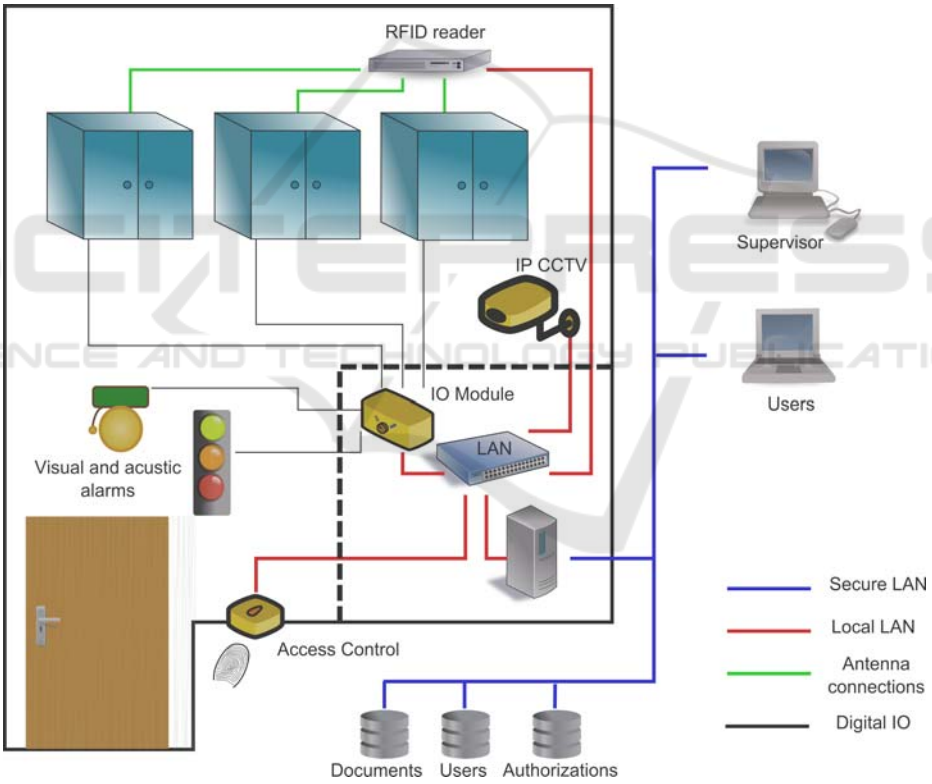

Fig. 1. System architecture.

Behind each cell, a HF RFID antenna has been placed. The antennas are powered whenever the doors of the related shelf are opened and are managed by Magellan MARS 24 RFID readers allowing:

– real time detection of document (or part of document) removal/replacement and related positioning in the archive,
– performing the archive inventory periodically, indicating if documents (or parts of documents) are present, missing and if they are in the correct cell.

User identification is performed through a fingerprint scanner (EFIS321 from ABS Applied Biometric Systems GmbH) allowing to authorized personnel to enter the archive room. As no more than one person can stay at a time in the archive room, the user identification device identifies who accessed confidential documents and when. One IP camera, whose image acquisition is triggered by motion detection, is used to monitor the archive. When anomalies are detected, i.e. a document is being replaced in the wrong position or a document for which an authorization has not been granted is being removed, visual and audio alarms are activated.

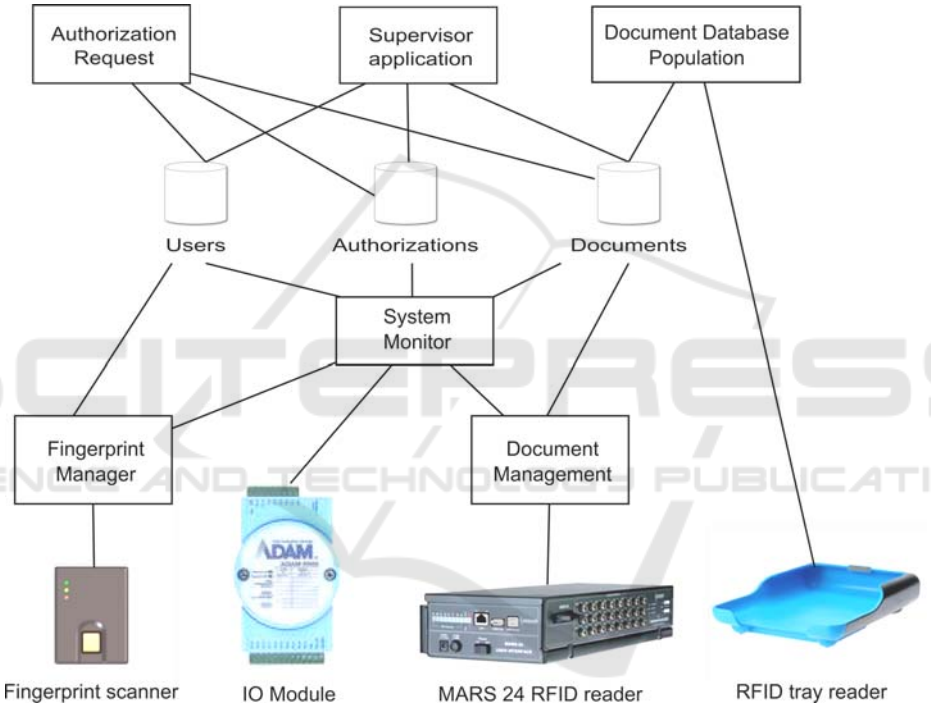

Fig. 2. Software architecture.

The software modules developed to manage the system components are shown in Fig. 2. The software modules synchronize their activities through socket communication exchanges and are the following:

Document Database Population. The document database population application is a useful tool to insert tagged document information in the document database. The application connects to the Document Tray Reader (a tray reader equipped with RFID antenna) and to the document database. The user inserts document information (document title, authors and date, number of pages, EU classification, position in the

archive, etc.) through a form; then, for each document page, the user is prompted to place the tagged document sheet on the tray, the related tag is read and the database is updated accordingly.

Authorization Request and Supervisor Applications. Two form based applications have been developed to respectively ask authorization to consult a document (Authorization Request) and to approve/reject requests (Supervisor Application). These applications update the database containing the authorization requests after having checked through the information contained in the user database that the person asking to consult a document has the appropriate credentials.

Fingerprint Manager. This module manages the fingerprint scanner. It allows to enter new users in the user database and it verifies user identity when a person tries to enter the archive room.

Document Management Application. This module manages the RFID archive, indeed it controls the Magellan Mars24 RFID readers connected to the antennas placed behind the bookshelves. The application receives from the RFID readers information on any tag that is found by the antennas or that goes out of the range of the antennas (expired). The application is configured to perform a logical mapping between the antennas and the shelf cells, allowing to know which documents are present/missing in the archive and in which position they are/should be.

The application is also aware of which tags belong to a document through the information stored in the document database. In this way the program updates continuously the state of the documents that are stored in the shelves. When a document is taken out, tags expire in groups. When one document is introduced, tags are discovered in groups. The program is able to detect when all the tags of a document are present, or when all the tags are out of range. In both condition a message is sent to the system monitor application through a TCP/IP connection, indicating which document entered or left the cabinet. To detect incomplete documents, the application uses a timer: all the tags that belongs to the same document should enter or leave the cupboard in a specific time lapse. If the application detects an incomplete document, it sends a special message to the system monitor application, specifying which pages are missing. The use of timers allows also solving the problem of “instable tags”. Indeed, when the quality of the tag is not very good, the signal is continuously detected and lost. Without a filter this instability would lead to a continuous “false alarm” messaging with the system monitoring application, as each time the message from a tag is lost it is considered that the related page has been removed from the shelf.

The software performs also a complete inventory of the document archive upon request (local request or from remote application). This feature can be also programmed in such a way that an inventory is performed periodically. The inventory result, organized by document, is sent to the system monitor application that compares the received information to the expected ones to detect any document missing or displacement.

System Monitor Application (SMA). This application is the core of the system. Through the user interface (Fig. 3) it provides a picture of what is happening in the restricted access area, performs all the checks needed to detect in real time anomalies

in the document management and records all the accesses and operations performed on the documents. A pane in the left part indicates the room status; in particular, it indicates the presence of a user in the room and her/his name, the status of the archive doors (locked/open) and the shelves that the user is authorized to open. To visualize these data, when a person enter the archive room, SMA needs to retrieve user data from the user database and document data from the document information database; then, with the retrieved data, SMA performs a cross check with the list of approved authorizations. On the right side of the screen there is a tabbed interface that shows all the available bookshelves cells and their content. The background becomes red if a document is missing or incomplete. On the bottom part of the screen there is a real time log of every event in the room. The same information is saved in a log file and verified in case of need.

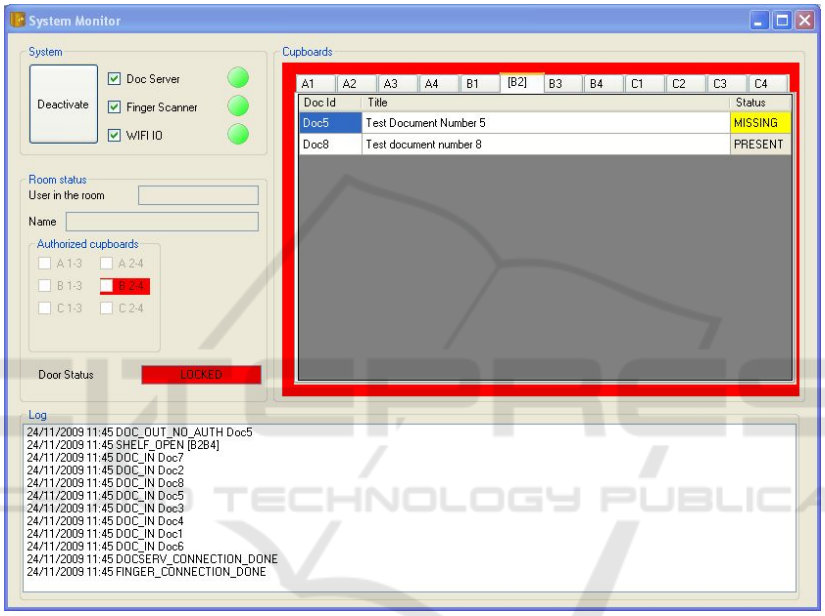

Fig. 3. System monitor application interface. A pane on the left shows the room status. A pane on the right shows the bookshelf cell status: archive position B2 is selected (see upper tabs) and the related content is visualized. As a document is missing the panel has a red frame.

3 Tests and Results

Two kinds of tests have been performed: document detection tests and functionality tests. Tags on document sheets were placed in such a way that they were perfectly overlapped and are programmed in such a way that they continuously answer when are in the range of field of the antennas (worst case scenario for tag mutual interference).

For document detection tests we considered three documents with different number of pages (8, 18 and 106 respectively) and we measured the range distances of the

RFID tags from the antenna (i.e. the back of the shelf) in which a document is correctly detected (100% COMPLETE), partly detected (INCOMPLETE) and not detected (100% MISSING). The results are reported in Table 1.

Table 1. Document detection performance.

Number of tagged pages	Document detection	Distance from the antenna [cm]
8	100% COMPLETE	<11.0
	INCOMPLETE	11.0-14.0
	100% MISSING	>14.0
18	100% COMPLETE	<7.0
	INCOMPLETE	7.0-10.0
	100% MISSING	>10.0
106	100% COMPLETE	<1.5
	INCOMPLETE	1.5-6.0
	100% MISSING	>6.0

For the functionality tests, a document database has been setup by tagging 8 documents for a total of 106 tagged sheets as shown in Table 2. The considered scenarios and the related expected system reaction are listed in Table 3.

Table 2. Document database for system functionality tests.

Doc ID	Number of pages	EU classification	Position in the archive
Doc1	16	TOP SECRET	A2
Doc2	14	SECRET	B3
Doc3	15	TOP SECRET	A4
Doc4	18	TOP SECRET	A3
Doc5	8	SECRET	B2
Doc6	10	TOP SECRET	A1
Doc7	15	CONFIDENTIAL	C2
Doc8	10	SECRET	B2

The standard procedure (Scenario 0) is the following:

1. The user asks the authorization to access a document for a given period of time
2. The supervisor validates the request
3. The user, in the right time window, enters the room after identification
4. The user opens the door of the shelf containing the document of interest
5. The user takes the document and read it
6. The user replaces the document in the original position in the shelf
7. The user identifies her/himself to leave the secure area
8. The system unlocks the door and the user leaves the room.

Each scenario has been tested at least 30 times by four different users: three users have been inserted in the user database, and the fourth was unknown to the system.

The only error occurred during tests was due to the fact that a known user has not been recognized by the fingerprint scanner.

Table 3. Tests scenarios and related system reaction.

Scenario	Description	System reaction
0	Standard procedure (see text)	Logging of all the operations
1	An unknown user tries to access the document room	Alarm generation
2	A known user tries to access the room without an authorization	Alarm generation. User ID is logged.
3	Authorized user tries to enter the document room in the wrong time	Alarm generation. User ID is logged.
4	The authorized user opens the wrong shelf	Alarm generation. User ID and shelf door coordinates are logged.
5	The authorized user takes the wrong document	Warning generation. User and document IDs are logged.
6	The authorized user replaces a document in the wrong shelf.	Warning generation and indication of the correct document position. User and document IDs, and document position are logged.
7	The authorized user replace an incomplete document.	Alarm generation and indication of the missing pages. User, document and missing pages IDs are logged.
8	The authorized tries to leave the archive when the archive is not complete (missing pages or documents)	Alarm generation and indication of the problem. User and involved document IDs are logged.

4 Conclusions and Future Work

In this paper we have shown the feasibility of integrating RFID technologies and security devices for the reliable management of sensitive document archives. There are still some open issues that need to be further investigated.

The first issue is related to the setup optimization, in particular for what concern the tag answering time. As mentioned in Section3, currently we have used the default setup (worst case scenario), with the tags answering continuously whenever illuminated. The used tags can be programmed in such a way to reduce the answering rate. For example, it would be possible to reduce by 4 the answering time of the illuminated tags; this is equivalent to reduce, theoretically, the active tag population to ¼ of the total amount making possible to have four times more tagged items placed inside a cell of the bookshelf without affecting detection performances. Regarding setup optimization, we expect that detection performances improve if tags of adjacent document pages are not overlapped. Next activity will therefore investigate the detection performance by varying the tag answering time and by changing position of tags in adjacent document pages.

Another issue regards the management of electronic document copies. In particular, there is the need to trace also document copies by logging who made the copy and especially to give only to authorized personnel the possibility to physically copy the document for which (s)he has the authorization. To solve this question, we are going to add to our prototype a commercial document scanner that will operate

only if the person using it has the authorization to copy documents. We will equip the scanner with an RFID antenna in order to verify that the copied document is exactly the one for which a copy authorization has been requested. The same adaptation will be done in the future for a copy machine working with tagged paper.

Acknowledgements

Authors wish to thank the colleagues from DG TREN, end users of the system, for the fruitful discussions on the procedures and rules in force for managing classified document archives.

Moreover, authors are particularly grateful to the colleagues of the SILab (Seals and Identification techniques Laboratory) for the provided support in implementing and testing the system; in particular, authors wish to thank François Littmann, leader of the SILab team, Michel Chiaramello and Graziano Renaldi.

References

1. Smart, L.: Making Sense of RFID. Netconnect (Fall, 2004)
2. Boss, R. W.: RFID Technology for Libraries. Library Technology Reports (Chicago: American Library Association, 2003)
3. Boss, R. W.: RFID Technology for Libraries, ALA Tech Notes. (2005)
4. NagaLakshmi, V., Rameshbabu, I., Lalitha Bhaskari, D.: A Security Mechanism for library management system using low cost RFID tags. Journal of Systemics, Cybernetics and Informatics, Vol5, No.1 (2007) 92-96