International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 4 (2012) pp. 144-152

Item Traceability Meets Human Traceability: Implications and Case Study

Ugo Barchetti, Luca Mainetti, Alessio Orlando and Roberto Vergallo

University of Salento, Department of Innovation Engineering
Via Monteroni, Lecce, Italy
ugo.barchetti@unisalento.it; luca.mainetti@unisalento.it;
alessio.orlando@unisalento.it; roberto.vergallo@unisalento.it

***Abstract*: The increasing attention by hospital and health bodies towards the issues related to devices, medical staff and patients identification and traceability is leading to the introduction of innovative systems, able to ensure access to medical reporting devices and, in the meantime, to guarantee the expected levels in terms of efficiency, configurability and upgradeability. Commercial solutions often do not satisfy these needs and cannot manage some important security issues in an efficient way. This paper presents a case study exploiting the RFID technologies and the EPCglobal standard for medical staff traceability in a real hospital context. Moreover, we present an implementation based on the Fosstrak framework, able to collaborate with an authentication system for digital signature on a Smart Card, satisfying timely intervention requirements and medical instrumentation data recording needs.**

***Keywords*:** EPCglobal, Human Traceability, Access Control, RFID, NFC, Track&Trace**.**

I. Introduction

Nowadays, hospitals and medical corps are focusing on instrumentation, medical staff and patient traceability technologies, as never happened before. The past decade has seen a rapid growth in the development and deployment of personal ID technologies for various market segments including civil identification, criminal identification, access control, attendance, surveillance, consumer identification and device/system access [1]. In this field of application, the RFID technology with the appropriate software represents a solution to information management in a more efficient and effective way.

Traceability is usually connected to the management of processes and activities aimed at item identification. For example, within supply chains an item has to go through electromagnetic fields in order to be identified and traced. In human traceability, instead, people can normally carry on with their activities being, at the same time, traced in a completely transparent way, without performing any special procedure.

Human identification and traceability will play a pivotal role in the interactions that people have with real-world objects, digital devices and business processes. The international market for biometric technologies is projected to increase from $3.4 billion in 2009 to $9.3 billion by 2014 with a compound average annual growth rate of 22.3 percent [1].

Our case study contemplates a first approach to medical staff traceability in a hospital context; this then combines with the issues related to the authentication and the use of the digital signature for medical reporting. For this particular context it is necessary to find a solution able to consider not only the intervention timing and the recording data needs but also the security requirements in terms of absence of interference between newly adopted and already in use instrumentation. The system, besides managing human traceability, will be intended for future traceability of all items and people related events.

This paper aims to give a concrete answer to the issues concerning human identification in a hospital context by means of the RFID technologies, avoiding any type of interference among instrumentation and, at the same time, speeding the medical reporting procedures.

We face these issues by referring to well-established standards, such as EPCglobal for operations traceability, which gives us the opportunity to link human processes to business transactions. Beside, in this paper, we want to demonstrate the applicability of a Track&Trace system, in which the relationship between antenna and tags is one-to-many, for human identification purposes, in which the relationship between antenna and tags is typically one-to-one (one reading device and one personal tag for each user).

The paper is structured as follows: in Section 2, a state of the art is reported, describing some solutions given by different authors to scenarios similar to ours. In Section 3, the case study scenario is presented. Section 4 gives a detailed description of the implementation framework with a focus on how EPCglobal has been extended in our particular context. Section 5 shows a critical evaluation of the proposed system taking into account the benefits and the limits in the observed case study. In Section 6, the conclusions summarize our key messages and sketch future research directions.

II. Related works

Several approaches to the issues of human traceability based on the use of RFID technology have been presented in different contexts by more than one author. The following paragraphs show how the RFID technology can solve problems linked to the efficiency and effectiveness of the security procedures in different environments, such as the hospital and the academic ones.

In [1], the author depicts the current needs of people authentication in India, where the lack of UID for 600 million poor people obstacles benefit and service fruition while encouraging frauds. The author reveal the use of multimodal biometric techniques as the key technology for personal identification, while enumerating some basic open issues like biometric data acquisition in rural areas, data theft and forgery and data storage architecture.

In [2], the authors describe the way how the new RFID technology can be employed to implement a “smart hospital” and they present some interesting applications, displaying promising perspective. By using open-source technologies, the authors prove the possibility to implement some of the presented use-cases. Authors, however, underline several problems to be solved before the health care community can adopt RFID technology in its whole potential: privacy managing, unintended wireless transmission of information related to the patients’ health conditions, interferences with the in use hospital instrumentation.

In [3], authors describe a prototypal system which involves the use of RFID tags and readers, developed to speed the log-in procedures to computers, manually configured by using the Microsoft Windows built-in functions. This system allows students to have access to the software they need from any computer station within the campus by means of some preferences recorded on the personal student identification card. It has been found that students taking part in the prototype testing have saved an average of 10 seconds by using the RFID login system instead of the traditional one. The authors strengthen this outcome suggesting the use of such a system in a hospital context: if a nurse saves 10 seconds in getting information about a patient, he/she can save 3 minutes for 20 patients and this value increases considering all the nurses activities in a whole working day.

In [4], the authors present the programming and implementation of an access monitoring and checking system based on RFID. This system, which allows the identification and authentication of people and objects, monitoring their access in private areas (such as laboratories), has a hierarchic structure: it detects the tags, takes a picture and sends the information to a server, which records the data and checks entrance permission on a database. When abuses or illegal actions are detected, a warning is sent to the surveillance guards. The experimentation results show that this system simplifies bureaucracy and automates the accesses to restricted entrance areas, raising the level of autonomy for the facility users (in this case, students).

In [5], the authors present an approach that permits an integration between the Supply Chain Management (SCM) and the software architecture of ID-Automation and which guarantees, in the meantime, the tasks division among the involved subsystems: a business message exchange system, implemented according to ebXML standard and a traceability system based on the EPCglobal standard. In this way, the authors demonstrate the possibility to obtain a drug history by questioning the web services of the companies belonging to the same supply chain. A chemist, for example, before a damaged pharmaceutical product, can read its EPC code recorded on the tag and, through the traceability process, can get to the steps that have caused the damage. Or, waiting for a lot of medicines whose delivery is late, knowing a priori its EPC codes it is possible to use the traceability system in order to get information about the lot updated route.

In [6], the author shows a way to give security access to a user equipped with a pre-authorized RFID tag. The tag must be within a maximum distance from an RFID reader to which it is coupled, integrated or linked by means of the information placed in a security committed database. If the identification code or other useful data contained in the tag correspond to the data saved on the security database, entrance is allowed to the user. A security access system of this kind can be used alone or together with other security systems, such as passwords, movable keys and biometric sensors. The authors think that requiring a limited physical distance between the user and a computer is necessary because a remote hacker cannot access the system.

In [7], authors describe a multi-layer health care system architecture for design of RFID-based Hospital Patient Management System (HPMS). Using HPMS, health care providers (e.g., hospitals) have a chance to track fast and accurate patient identification, improve patient’s safety by capturing basic data (such as patient unique ID, name, blood group, drug allergies, drugs that the patient is on today), prevent/reduce medical errors, increases efficiency and productivity, and cost savings through wireless communication. The HPMS also helps hospitals to build a better, more collaborative environment between different departments, such as the wards, medication, examination, and payment ones.

In [8] the author proposes an authentication framework called Authentication Processing Framework (APF), that makes it compulsory for the readers to authenticate themselves with the APF database before they can access registered tags. The APF provides assurance, to the RFID users, that the information stored in the tag is secured in the sense that only authenticated reader by the APF can have access to the tag. The reason for this is that the information received by the reader from the tag is encrypted and can only be decrypted by getting the decryption key from the APF. Also, the reader that did not register with the APF before getting the information from the tag will be denied of getting the decryption key. The reason for this is in order to circumvent malicious readers from accessing tags illegally. This framework is designed for read only RFID system.

In [9] authors present a system which supports the operation of an analyses laboratory. Introducing the use of contactless smartcard they improve the usability of the system speeding the existent slow authentication process based on login and password typing. The deployment of the system at the laboratory was implemented on two main points. On the first one, the system receives and records the requests of both direct examination of the doctors stations and the laboratory reception. These procedures can be performed through the use of smart cards with RFID. On the second one, the system makes the identification through the RFID tags attached to the tubes of collections for clinical examinations and the bracelets for identification with RFID placed on the arm of hospitalized patients.

The performances of health monitoring systems are really important, as described in [10], where the authors present the results on the performance of a WSMN (Wireless Sensor Mesh Network) used for patient health monitoring application, in terms of parameters like delay, MAC delay and throughput under varying number of patients and varying number of doctors in wards and also the failure performance when the mesh nodes fail based on simulation study carried out with OPNET Modeler 15.0. The WSMN was born from the integration of Wireless Mesh Networks (WMN) and WBSN Wireless Body sensor Network. In this scenario, WMN can be used to transmit vital information arising from the wireless Body sensor Network (WBSN) to the backbone

network, while the wireless body sensors can then be configured to convey the patient's status directly to the assigned doctor/nurse through the personal smart phone, PDA or Palm device. In the simulation scenario has been observed that increasing number of in-patients may not pose that severe problem in the delay performance of the whole network.
Another human identification approach is described in [11], where the authors propose an autonomic wireless sensor/actuator networks that classifies a user's behaviors in relation to environment control such as lighting, and that configure themselves depending on sensor node selection. Authors demonstrate tracking environment control behaviors and sensor node selection using a sensor network test bed. First, they have used an Self Organizing Map (SOM) to visualize the relationship between the responses of nodes. Next, they have evaluated the sensor node selection and network reconfiguration. Based on the information gain criterion, the informative sensor nodes for behavior classification were successfully chosen without sacrificing the classification performance. The proposed sensor/actuator networks can be useful for constructing an automatic energy-saving environment control system adaptive to the user's behaviors.
Another similar approach is [12] where the authors propose a distributed soft sensors network, examining the hybridization with Neural Networks (NN) and Wireless Sensor Networks (WSN) into a Smart Home application, called Smart Table. This appliance is interesting as a case study because it requires distributed processing and representation, pattern recognition and pattern classification, which are advantages inherent of WSN and NN applications. The mapping and hybridization of these networks provide benefits, such as, reduction of the time of prototyping and composition of the system in a smaller number of activities. Preliminary prototypal results presented by the authors show that Multilayer Perceptron is a good candidate for using into low-cost System-on-a-Chip (SOC) such as Peripheral Interface Controller (PIC) microcontrollers.
From the analysis of the listed works, it is evident the necessity of defining a fast access to services and an identification system which, despite the use of the RFID technology, would take into account the surrounding environment, producing the least possible interferences with any type of in use instrumentation.

III. Case study

Studying a strategy for automatic medical reporting, one of the most common problems concerns the need to have an integrated management of both digital signatures and medical reporting support services.
Hospitals and first aid centers have to cope with daily challenges, mainly in emergency cases. Medical staff must manage a large number of patients at the same time, in an effective and efficient manner, hence the need to quickly locate the medical staff and the suitable devices for rapid interventions. The same rapidity is required in the medical reporting and administrating procedures concerning patient's case histories. In this intervention field there is the need to overtake an impasse related to the digital signature management. This impasse is always due to the unsuitability of most of the products intended for this purpose because they offer a range of functions that are not always useful to digital signature management. Within a context where the timeliness of intervention is a key element also in the most common and simple cases, arises the gap among the solutions available on the market and the actual needs.
Let us consider the following scenario: a man is involved in an accident and has a strong leg pain. The hospital stay starts with the emergency arrival in the first aid ward; after recording the patient medical history, the first aid doctor takes X-rays of the patient's lower limb. On the base of the X-rays result, the doctor considers the necessity to admit the patient, in order to carry out more tests. During the hospitalization, more tests and checks are carried out on the patient's limb and all the doctors working on the patient create, read and update several reports, containing important data about his health.
In such a situation, intervention quickness can be vital, also in the data recording; using an application which requires the input of username and password in cases when, for example, a charge nurse, has to measure and record temperatures during the check rounds, can lead to a waste of 20 seconds for each patient for log-in procedures, with an incremental loss of time.
The use of RFID technologies in hospital and medical contexts opens new perspectives in terms of objects and, most of all, people traceability. The possibility to trace movements and actions of medical staff within a hospital would lead to a higher reliability both for patients and the whole facility, bringing more efficiency and effectiveness into the internal working procedures.
The use case related to digital signature is one of the several aspects that can be object of traceability; although this use case regards a particular aspect of most cases, it appears clearly the need to implement a system able to be scalable and upgradeable for the future aims, using a software and hardware instrumentation which would not interfere with the ongoing activities and, mainly, with the operating medical instrumentation in use. Extra-domain technologies have been introduced in order to overcome the limits of the current digital signature support systems: for some operations the current solutions on the market are so slow that they can also get to the range of 20 seconds waiting.

IV. Integration and implementation architecture

Taking into account the requirement of non-invasiveness, we have designed a flexible and highly configurable architecture and developed the related authentication and access tracking system using smart cards equipped with RFID tags. The traceability has been obtained by using the open source platform Fosstrak [13] based on the EPCglobal Standard [14]. In the architecture analysis shown in Figure 1 we distinguish the server side from the client side. In particular:

- The Host client embeds the HTML login form, the smart card reader driver installed on the operating system, and the library, which allows to interface the browser with the device.
- The Track&Trace server provides the Fosstrak framework structured on a multi-level architecture. In particular it is used to capture, filter, process and store data detected by the readers.

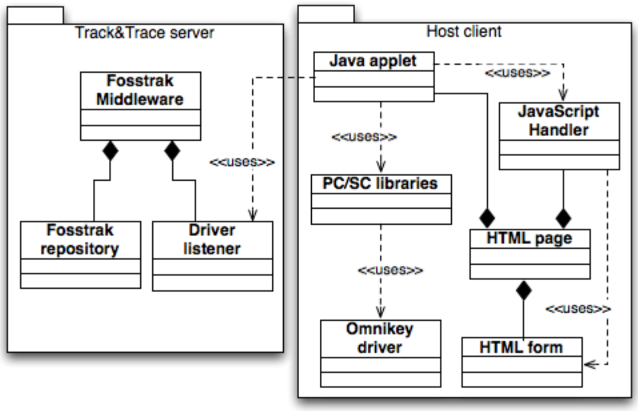

Figure 1. System architecture

The Fosstrak framework is installed on the Apache Tomcat 6.0 Application Server, while the Fosstrak repository uses the MySQL 5.0 DBMS.

A. Adopted technologies

The made technological choices are based on the need of fast identification (order of magnitude of few seconds) and on a short range of action during the recognition (order of magnitude of few centimeters). This last requirement comes from the need to avoid every kind of interference with the medical instrumentation (if present). Therefore an integration of an HF chip (ISO 15693 13.56 MHz) in every company badge (contact smart card) has been foreseen. The use of the NFC (Near Field Communication) technology for the identification and access to an existing application was also adopted in order to avoid the number of false reading, as a narrow proximity is necessary (around 2-3 cm) for a tag to be detected. According to the previous described choice, the actual will of the user to be identified is needed: a staff member who walks at a distance of 2-3 meters from the computer probably does not want to access it, and surely does not accept that his identification code could be displayed on the screen without his explicit will. As a consequence of this choice, we have identified a contact and contactless card reader suitable for the hospital context. We have chosen the USB reader Omnikey Cardman Reader 5121 [15] which has demonstrated to not interfere with the medical equipment.
The tracking and tracing system, inside the hospital facility, concerns at present just the login procedure made by the staff after the identification of their respective transponders. Considering the possibility of future developments, we have decided to adopt the EPCglobal standard, leader for the factory oriented standard development for the Electronic Product Code (EPC). As an EPCglobal standard implementation, we have chosen Fosstrak, an open source platform for RFID-oriented software, which provides supporting components for the development and integration of Track&Trace applications.

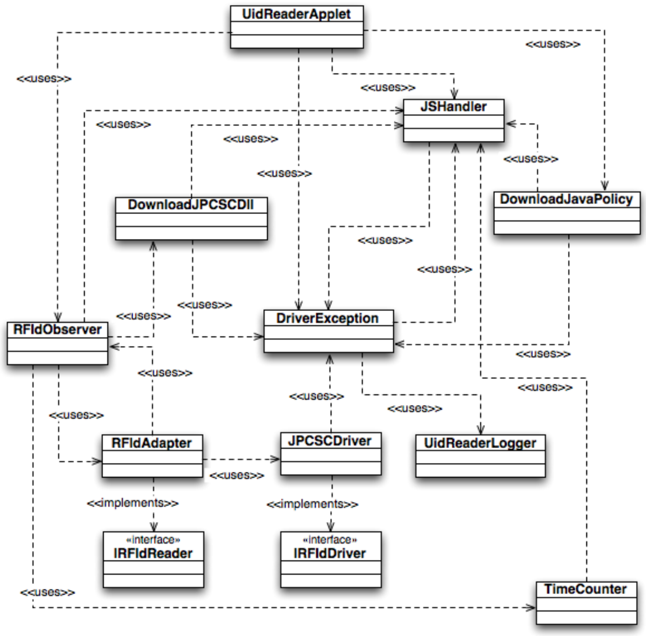

Figure 2. Client-side software architecture of the solution

B. Client side

The Client task is to put in communication the Omnikey Cardman Reader 5121 device with the terminals located in the various hospital wards. This task prefigures the implementation of an adapter able to obtain the identification code stored in the smartcard HF chip using the Omnikey reader.
In order to confer easiness of use, flexibility and scalability to the whole system, and for an optimized management of the large number of clients, the implementation of a single Java applet has been chosen as the proposed solution for extracting data from the reader. The applet deals with the communication between the browser and the Track&Trace system handling data derived from the detected smart card readings. Such a solution allows the user to use just one application on each client making him/her free from any possible problem deriving from installations and upgrade needs.
In order to allow communication between smart card reader and the host client, we have selected the *jpcsc* library [16] provided by IBM, which allows Java software to communicate with PC/SC [17] compliant smart card readers; PC/SC is the communication standard for smart card readers and PCs.

C. Server side

The traceability system has been implemented by the use of the Fosstrak open source platform.
As shown in Figure 3, Fosstrak fully implements the multi-level stack described by the EPCglobal standard. We can distinguish:

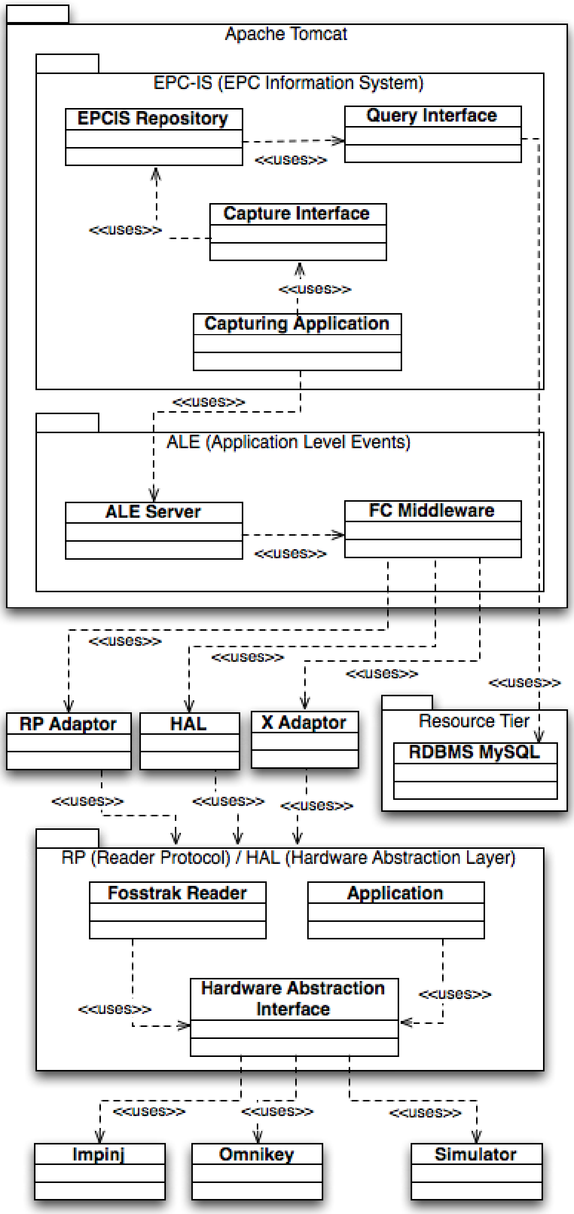

Figure 3. Fosstrak multi-layer architecture

- The RP level [18] which implements the Reader Protocol Standard dedicated to the interaction with devices able to read or write EPC tags.
- The Filtering and Collection Middleware level [19] which implements the Application Level Events standard. This level implements an interface through which the various clients can obtain filtered and consistent EPC data incoming from a great variety of sources.
- The EPCIS (EPC Information Service) [20] which aims to allow several applications to handle EPC data though EPC-related data sharing within and outside the firms.

The event data registered by reader is sent to Fosstrak and, step by step, filtered and enriched with a business semantic along the three previously explained levels. The reading event (in particular, the medical staff smartcard reading obtained via the Omnikey reader) is finally registered in the Fosstrak Resource Tier represented by the EPCIS Repository.

D. Implementation

Referring to the proposed architecture, we have implemented a driver that allows the communication between the applet and the Omnikey reader. The reader, previously installed on the client, interprets the PC/SC commands. The application uses the jpcsc libraries that wrap a dll library copied into the client's file system at the first run by the same application.
The approaching of a card to the reader fires a proximity event which carries out the UID code recorded on the card; once the UID is obtained, the applet displays it in the login form through the JavaScript code generated at runtime in the containing html page.
The software architecture of the driver interconnecting the Omnikey reader with the web interface, is based on 3 different design patterns, that make the application effective, efficient, modular and scalable:

- The Observer pattern [21] which has been used to create a listener class subscribing to the services of an observable class, whose task is to interrogate the RFID reader device; the observable class notifies new reading events to the listener objects subscribed to its service; in this way we avoid the use of constant polls;
- The Adapter pattern [21] which has been used to provide an abstract solution to the problem of extendibility for future interfaces. Using this pattern, it can be faster and easier to switch to a new library version or a completely different technology for device interrogation;
- The Singleton pattern [21] which guarantees that one and only one instance of the physical reader communicating class will be created.

E. UID code mapping

To obtain a fully EPCglobal-compliant architecture we have had to re-map the 16 digit coding of the RFID tag applied to the hospital employees' smart cards. The choice among all the different kinds of EPCglobal compliant formats has fell to SGTIN-198 [21], which is the only one that reserves a serial number field large enough to represent the 16 digit identification code contained by the HF tag.
The fields representing the company prefix and the item reference category defined by the SGTIN code have been used with a default value of 0. In this way, whenever the hospital firm will take into account to join a larger EPCglobal network, it will have to request its own company codes that could be used to identify the different wards, the employees qualification level or the equipment types.

F. Integration with Fosstrak

The HTTP protocol is used to transmit the UID code read from the smartcard, therefore the integration with Fosstrak introduces an anomaly compared to the usual TCP socket communication between the RFID readers and the Track&Trace server. To receive the red identification codes, a servlet supporting Fosstrak's Hardware Simulation Layer has been developed. The servlet works over HTTP as an online driver/adapter.
As can be seen from the Figure 4, Fosstrak and the Omnikey readers communicate with each other through two essentials actions: on the one hand the servlet instance of the Omnikey adapter listens the tag readings over HTTP and fills up the UidBuffer with captured UIDs; on the other, the

OmnikeyBufferReader object forwards all the readings from the temporary buffer to the EventCycle Fosstrak's object through the OmnikeyAsyncIdentifyListener object. Then Fosstrak forwards the information to the next levels, adding a business semantic to the data and finally storing them into the EPCIS Repository.

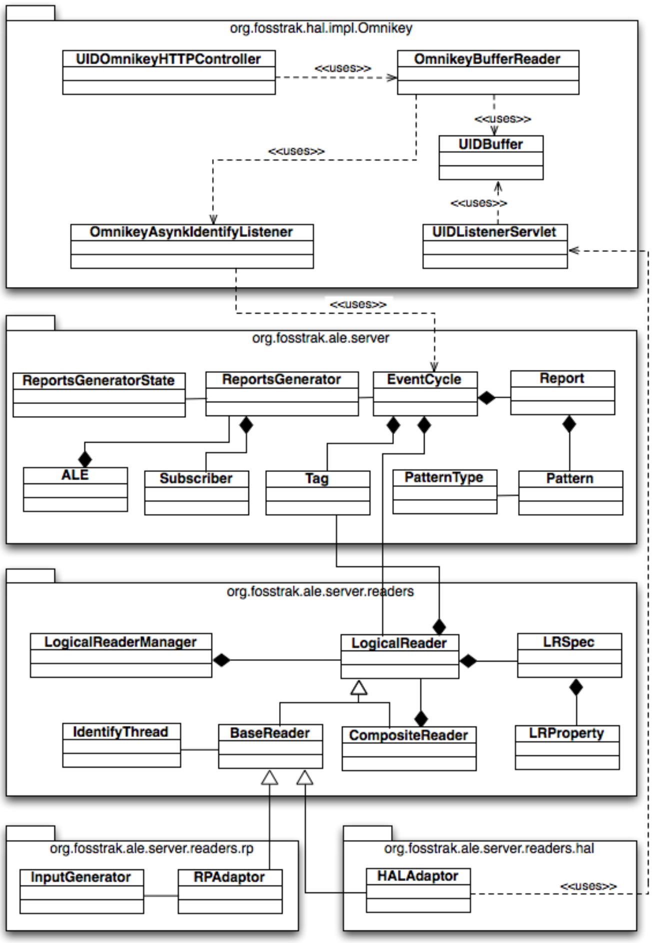

Figure 4. Interconnection between Fosstrak and the online driver/adapter

The UidBuffer thread-safe implementation allows an optimized management of the contemporary readings incoming from the host clients.

G. *Capturing application*

The Fosstrak Capturing Application generates the event objects to be stored into the EPCIS repository; it listens over a socket connection from which it receives the reading events incoming from the Filtering and Collection layer stored in the ECReport xml files.
The Capturing Application represents the bridge between the Fosstrak's event management layer and the business logic layer represented by the Fosstrak EPCIS.
In previous related works [23] we have needed to separate the receiving feature of ECReports from their following processing, for the reason that a particularly onerous ECReport (e.g. thousands of red tags) may cause a serious resource overload, generating a connection buffer saturation. This will consequently bring losses of ECReport (lost readings). Our solution consists of decoupling the receiving and processing functionalities. We have implemented a listener class working with a TCP socket, which reads and saves the incoming ECReports into a MySQL buffering table. This last implements a FIFO queue and it is managed in parallel by the handler object which reads, processes and deletes the oldest element from the queue.
This approach, also applied to the presented case study, provides reliability and robustness to our Capturing Application.

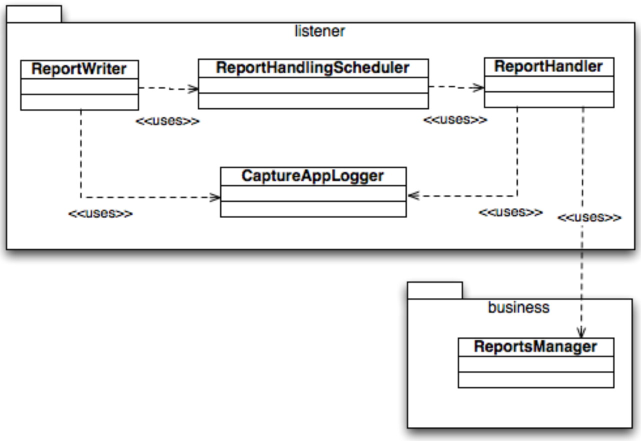

Figure 5. Software architecture of the Capturing Application

V. Evaluation

In this paragraph we present a critical evaluation of the proposed system taking into account the solved problem, the benefits arisen during the system test and the corresponding limits. Finally we summarize all these aspects in Table 1. This analysis can be useful to evaluate the adopted solution within the hospital context.

A. *Solved problems*

The introduction of the EPCglobal standard and its implementation (Fosstrak) has brought us to face with two issues related to the design and the implementation steps.

1) *Topological problem.*

Fosstrak, when is used with the default configuration, polls the readers that are singularly pointed by each configuration file using the abstract concept of Logical Reader. In this way, Fosstrak can correctly handle the captured tags, mapping such readings with the known IP addresses and consequently with the readers which provides these data. In our case study the scenario presents an anomaly: Fosstrak listens upon a single HTTP connection, and only by this it will receive all the reading events coming from thousands of USB readers placed around the hospital. Such a quantity of readers would normally request the same number of similar configuration files that differ each other for the IP addresses of the hosts to which the readers are connected. Besides, taking into account that IP address is useless because Fosstrak cannot directly poll the readers, we have chosen to denormalize the topology supported Fosstrak: we have considered the whole hospital identification system as a single Logical Reader made up of all the smart card readers; each reader works as a singular antenna referring to a single virtual reader represented by the servlet. The readings captured by the servlet show to the system both the read UID and the host IP. The information

UID+IP moves along the Fosstrak middleware until the Capturing Application receives it.

2) The multiple readings problem.

An Event Cycle strictly related problem is that the Omnikey Cardman Reader 5121 fires a single reading when each RFID tag is detected; on the contrary, the classic supply chain instrumentations fire multiple readings for the same item during a single Event Cycle. The risk while using the Omnikey reader is to lose some readings when the UID code is received outside the reading collection period specified by the Event Cycle duration period parameter. We solved this problem by implementing a multiple readings server-level simulation: we simply send artificially repeated readings to the Fosstrak Event Cycle object. The UID code repetition period can be conveniently adjusted setting the proper parameter contained in the server application configuration file.

B. Benefits

The main benefits obtained by the use of our EPC-aware human traceability solution are listed below.

- The system deals with the human identification requirements offering the benefits of an EPCglobal standard Track&Trace solution. This means that the system not only offers the possibility to control authorized user accesses, but also to trace their activity for further analysis.
- The system overcomes the limits imposed by the existing commercial solutions, which lead to an incremental loss of time also for the simplest procedures. This is a strong advantage, especially within a context where the timeliness of intervention is a key element for saving human lives.
- The client side has been designed as a plugin, so it is quite easy to integrate it within more complex systems.
- The system can be customized for different identification methods, e.g. UHF RFID tags or 2D barcodes, by simply implementing a custom driver compatible with the provided interfaces.
- The out-of-the-box system (with HF tags and readers) is proved to be usable near high electromagnetic emission instrumentation without any problems for people.
- The system is highly scalable and supports the extension towards a bigger network thanks to an accurate software architecture design.

C. Limits

Here we list the main limits of our solution, taking into account of the specific case study we have presented in the Section 3.

- Our system lacks a security layer responsible to avoid RFID frauds when logging into the system. Nevertheless unrecognized UIDs cannot access the system and the applet behavior is unknown when different HF tags (e.g. ISO 14443 A-B compliant tags) are red by the Omnikey reader. Besides, the servlet exposed by the traceability server does not require authentication; this is an important vulnerability leak.
- Having we used a self-signed certificate for letting the applet access to the client system, a non-expert user could get confused by the applet security notice. The user has to trust the identity of the applet's signer when loading the applet for the first time; this can frighten non-expert users or leading them to trust similar notices on different unsecure applications.
- We haven't implemented any specific redundancy technique for the Track&Trace server, so it represents a system's single point of failure. Consequently, if the server is down, the login activity cannot be registered.

The following table summarizes the evaluation results explained above.

Solved problems	**Benefits**	**Limits**
Topological problem	Track&Trace of identification activity	Lack of a security layer for the RFID tags trusting
Multiple readings problem	Minimization of identification times	Possible security leaks accessing client system within a web browser
	Possible integration within more complex architectures	Track&Trace server is a Single Point of Failure
	Possible use of different identification mediums	
	Compatible with high-emission electro-magnetic instrumentation	
	Scalability	

Table 1. Evaluation summary

VI. Conclusions

In this paper we have presented a case study on medical staff traceability in a hospital context, with a critical eye on the integration with the authentication functionality and the digital signature usage in medical reporting. We have presented moreover a system, based on the EPCglobal standard, capable of handling human traceability related events. This system can support human identification through a customization of Fosstrak system in which the relationship between antenna and tags is typically one-to-one. We have evaluated benefits and limits of our proposal; in this evaluation we have identified two main problems: a topological one and one more related to multiple reading problems. Then we have detailed the arisen benefits and the related limits verified during the testing phase.

Future work will be devoted to extending the traceability framework to all the events related to persons and things, and to integrating the proposed system with the Health Level Seven standard (HL7) in the pharmaceutical field, exploiting the Electronic Patient Record (EPR) in innovative application scenarios.

Acknowledgment

We would like to thank "WebScience srl", an italian company that contributed and funded our research within the *Identify* project.

References

[1] K. Ricanek. "Dissecting the Human Identity", *Computer*, XLIV (1), pp. 96-97, 2011.

[2] P. Fuhrer, D. Guinard. "Building a smart hospital using RFID technologies". In *Proceedings of the 1st European Conference on eHealth*, pp. 131-142, 2006.

[3] K. Galitz, et al. "Using Radio Frequency Identification (RFID) to bring up user preferences and decrease login time across networked computers". 2005.

[4] F. Lourenço, C. Almeida. "RFID based Monitoring and Access Control System". In *Proceedings of the 15th conference on Professional Information Resources (INForum 2009)*, pp. 203-214, 2009.

[5] U. Barchetti, et al. "Supply Chain Management meets Auto-ID Management: A Structured Approach". In *Proceedings of the 17th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2009)*, 2009.

[6] S. Dean. "System and Method of using RFID tag proximity to grant security access to a computer". *Patent Application Publication US20090210940*, Intermec IP Corp., Everett, WA, USA, 2009.

[7] B. Chowdhury, et al. "RFID-based Hospital Real-time Patient Management System". In *Proceedings of the 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)*, pp. 363-368, 2007.

[8] J. Ayoade, "Security implications in RFID and authentication processing framework", *Computers & Security*, XXV (3), pp. 207-212, 2006.

[9] G. Florentino, et al. "Hospital Automation RFID-Based: Technology Stored In Smart Cards". In *Proceedings of the World Congress on Engineering (WCE 2008)*, pp. 1692-1695, 2008.

[10] N.A. Benjamin, S. Sankaranarayanan. "Performance of Wireless Body Sensor based Mesh Network for Health Application", *International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM)*, II, pp. 20-28, 2010.

[11] M. Nakamura, et al. "Autonomic Wireless Sensor/Actuator Networks for Tracking Environment Control Behaviors", *International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM)*, I, pp. 125-132, 2009.

[12] S. G. Soares, et al. "Building Distributed Soft Sensors", *International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM)*, III, pp. 202-209, 2011.

[13] "Fosstrak Free and Open Source Software for Track and Trace", *http://www.fosstrak.org/*, Auto-ID Labs, Zurich, Schwitzerland.

[14] "EPCglobal Standards Overview", *http://www.gs1.org/gsmp/kc/epcglobal*, GS1, Brussels, Belgium.

[15] "Smart Card Readers for Logical Access Control - HID Global - OMNIKEY Readers", *http://www.hidglobal.com/technology.php?tech_cat=19&subcat_id=10&headerType=1*, HID Global, Irvine, California, USA.

[16] "MUSCLE - Cross-Platform Smart Card Development", *http://www.linuxnet.com/middle.html*, Linuxnet, Newark, New Jersey, USA.

[17] "PC/SC Workgroup Specifications Overview", *http://www.pcscworkgroup.com/specifications/overview.php*, PC/SC Workgroup, San Ramon, California, USA.

[18] "Reader Protocol (RP) Standard", *http://www.epcglobalinc.org/standards/rp/rp_1_1-standard-20060621.pdf*, GS1, Brussels, Belgium, 2006.

[19] "Application Level Events (ALE) Standard", *http://www.epcglobalinc.org/standards/ale/ale_1_1-standard-core-20080227.pdf*, GS1, Brussels, Belgium, 2008.

[20] "EPCIS - EPC Information Services Standard", *http://www.epcglobalinc.org/standards/epcis/epcis_1_0_1-standard-20070921.pdf*, GS1, Brussels, Belgium, 2007.

[21] E. Gamma, et al. *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley Professional, Redwood City, USA, 2007.

[22] "EPC Tag Data Standard (TDS)", *http://www.epcglobalinc.org/standards/tds/tds_1_3_1-standard-20070928.pdf*, GS1, Brussels, Belgium, 2007.

[23] "TRUE Project", *http://www.trueproject.unisalento.it/*, Department of Innovation Engineering, University of Salento, Lecce, Italy.

Author Biographies

Ugo Barchetti Ugo Barchetti graduated in Computer Science Engineering from the University of Salento (Italy) in October 2002 where he received a PhD in Computer Science in September 2007. His research interests include virtual collaborative learning management systems, service oriented architecture, web design methodologies, business process design, business notation, interoperability techniques and business driven integration. He took part in several international research projects regarding the development of collaborative virtual experiences for e-learning purposes and middleware tools in order to support B2B exchange and supply chain management. He is co-author of several international scientific papers.

Luca Mainetti Luca Mainetti is an associate professor of Software Engineering and Computer Graphics in the Department of Innovation Engineering at the University of Salento (Italy). His research interests include web design methodologies, notations and tools, web and services oriented architectures, and collaborative computer graphics. He is scientific coordinator of the GSA Lab { Graphics and Software Architectures Lab (www.gsalab.unisalento.it), and IDA Lab { Identification Automation Lab (www.idalab.unisalento.it). He is Rector's delegate to the ICT. He received a PhD in computer science from the Politecnico di Milano (Italy). He is a member of the IEEE and the ACM. He is the co-author of more than 80 international scientific papers.

Alessio Orlando Alessio Orlando is final year student in Computer Science Engineering from University of Salento (Italy) and collaborator of the GSA Lab { Graphics and Software Architectures Lab (www.gsalab.unisalento.it), and IDA Lab { Identification Automation Lab (www.idalab.unisalento.it). His study activity concerns with the designing and developing of traceability oriented architectures by the mean of RFid technologies. He has acquired specific skills in the use of EPC Global standard and open source traceability frameworks in the Supply Chain Management field. He enjoyed many research projects in the study and optimization of goods and human traceability systems.

Roberto Vergallo Roberto Vergallo graduated cum laude in Computer Science Engineering from the University of Salento (Italy) in October 2010. His research interests include service oriented architecture, interoperability techniques and business driven integration, Near Field Communication, Internet of Things and mobile ubiquitous systems. He took part in several research projects regarding the development of middleware tools in order to support B2B exchange, supply chain management and healthcare interoperability.