Mobilizing Business Processes Security Issues and Advantages of Using Sap Mobile Infrastructure In The Development of Mobile Applications

Ilona Mariana NAGY[1], Laszlo FEISCHMIDT[2]
[1]Babeş-Bolyai University of Cluj-Napoca,
Faculty of Economics and Business Administration,
[2]MSG Systems Romania, Cluj-Napoca
Mariana.Nagy@econ.ubbcluj.ro,
Laszlo.Feischmidt@msg-systems.com

Nowadays the world is confronted with an increasingly mobile and information-driven environment. Companies are trying to adapt to the new trend and face the challenges by extending their traditional business making procedures with mobile solutions, in other words they are attempting to mobilize their business processes. Encouraging the development of mobile applications has proved to be a wise decision on the behalf of various companies with initiative since a rather considerable amount of time in the "doing business" action is spent underway. Transitioning to this mobile environment raises some security issues though, as a company's internal data must be kept private and undisclosed to the public eye and especially protected from external as well as internal security attacks. The goal of this paper is to present the advantages, when it comes to security questions, of using an integrated mobile infrastructure for the implementation of a car insurance claims handling mobile system. The study reported in this paper is designed to cast some light on the new SAP concept called SAP Mobile Infrastructure by comparing the architecture and security "advantages" to a similar development infrastructure.

Keywords: *business processes, mobile infrastructure, security aspects in mobile applications, SAP mobile technology*

1 Introduction

In order to understand the necessity for a company to extend its business processes on mobile applications, we must first define the underlying terms. A business process is in fact a collection of interrelated processes - a set of linked activities that take an input and transform it to create an output [1] - functioning in a logical sequence to achieve a predefined goal. Davenport's definition refers to a business process as being a specific ordering of work activities across time and place, with a beginning, an end, and clearly identified inputs and outputs: a structure for action (Davenport, 1993). According to this definition a process must be comprised of several activities ordered in time and space, clearly defined; within the company this transformation of an input into an output must add value and in the end the customer must benefit from the outcome.

In the specialty literature we can find a distinction between three types of business processes: management, operational and supporting processes. This paper will refer mostly to the first two types: the processes that conduct the operation of a system and the ones that represent the core business. As the essence of an organization, business processes define how the internal activities are being executed by means of people and IT infrastructure. For this reason, companies are automating and mobilizing them, achieving as a result an improvement in time response, operational efficiency and business agility. Extending a company's activities with mobile technology (where most of the human interaction is done using mobile devices) is known as "mobilizing" the business processes [2].

2 Mobile business processes

The mobility of a business process is achieved when one of the following conditions is met: there is an uncertainty of physical location, this uncertainty of location is externally determined and from the process point-of-view, cooperation with external resources is needed in the execution of the business process [3].

This mobilization brings certain advantages to a company's processes. The main benefit is the enhanced efficiency of its location-sensitive and time-critical activities. This also includes the reduced operational and transactional costs, the improved service quality and the increased customer satisfaction. All these advantages are primarily gained through the increased speed of the business reporting that supports the decision-making process. The security issues regarding the "mobilization" of the business processes come to mind whenever a company is taking into consideration their extension. This represents a major drawback for the mobile business promoters, as they depend extensively on the technological achievements and progress. Companies that use mobile devices for the development of their business processes should consider some recommended mobile security measures and practices such as: power on authentication, file encryption on the mobile device in order to prevent unauthorized data disclosure, backup and restore for protection against data loss, communication over secured network and trusted channels to avoid security attacks, etc.

2.1 IT Scenario for a Mobile Business Process – Case study

The registration and management of the car insurance claims in the SAP system is handled with the help of a transaction module which, upon launching, enables the recording of the claims into the system and distributes the newly registered ones among the inspectors. The insured event implies a lengthy process which in the end can result into the victim's material gratification. It begins with the completion of the official documents required by the insurance company for starting the compensation process, at the scene of the accident. At the insurer's office this information will be stored in the database system from where it is distributed among the existing inspectors – each agent will receive a notification through an email client-like user interface, decide on the validity of the claim and proceed to the accident scene for further verification and assessment. Upon the completion of the official documents, the given claim's information will be modified in the system.

This process, from the inspector's point-of-view is exemplified in the following figure (Figure 1.):

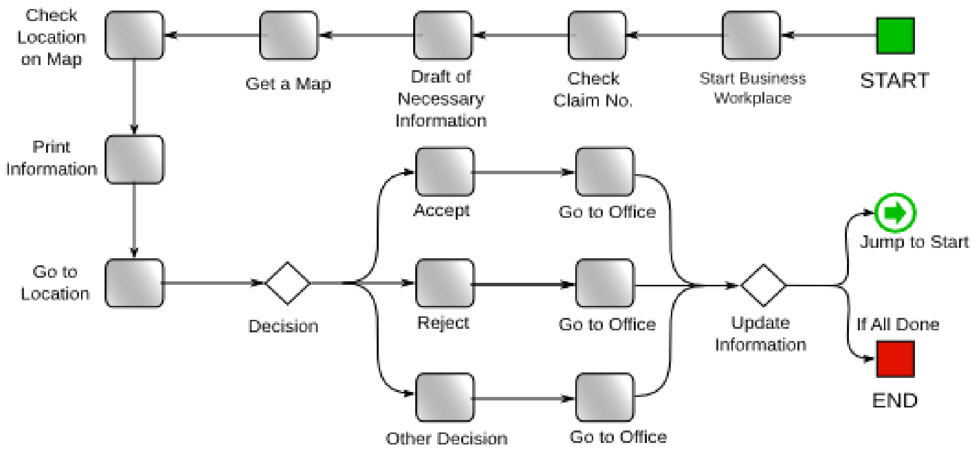

Fig. 1. Claims registration process

Each inspector must logon to the system and verify its assigned claims, go to the accident scene, write a report and return the data into the system.

This rather complex and time consuming chain of activities can be reduced to a more efficient process which involves only the inspector and a mobile device by which he can register the insurance claims remotely. Facilitating the inspector's work, while reducing the company's operational costs, represents a target for the any insurance company, therefore a mobile application that meets these goals has a high chance of success on the market place. The following figure shows the mobile solution for the insurance claims registration process:

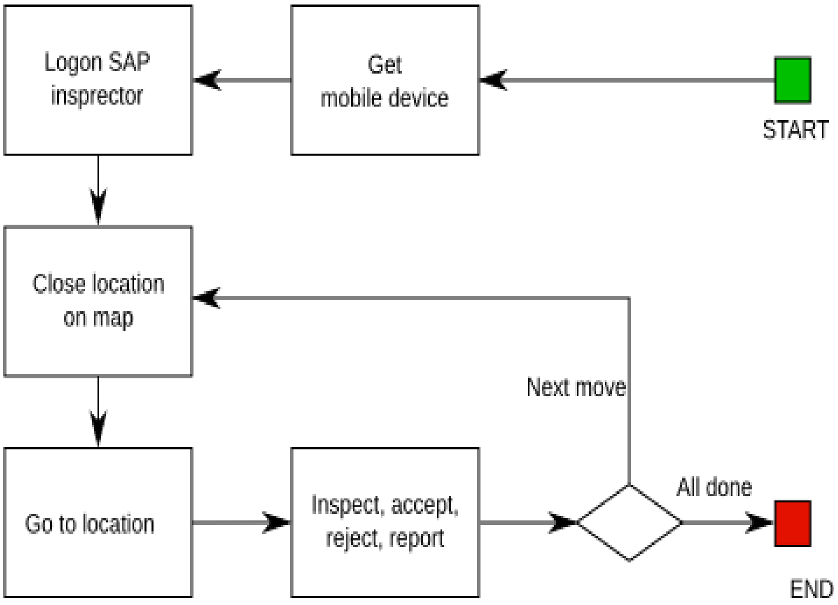

Fig. 2. Mobile Inspector

The chain was trimmed as it follows: the inspector has a mobile device that he uses to logon to the SAP inspector system where he can see all the reported accidents locations. He chooses a location on the map (the decision factors for his choice are irrelevant to this case study) and goes to the selected location. He inspects the causes of the accident, reports the findings to the system and decides whether to accept or reject the claim. Next, he can end the process chain or go to another location. Due to the trimming of the process chain, it can be easily concluded that the main advantages of using the Mobile Inspector application are the reduced operational costs and the time saved for the company.

2.2 Technologies used for implementation of Mobile Inspector – Security issues

Following the description of the mobile application from a business point-of-view, we will now focus on the implementation technologies used and especially on the security issues emerging from them. The technologies used for the development of this mobile application are: the Android operating system for the mobile device, the Glassfish application server for Java Platform Enterprise Edition, the SAP Web Application Server and the SAP Database Server.

The Android operating system is a Linux platform programmed with Java that runs on mobile devices and has the same capabilities as a regular operating system: efficient memory allocation for the run processes, multitasking, a file permission system and UIDs (UNIX user identification). Android has a unique security model (process isolation) based on the concept that each application runs in a different UID, given upon installation, in contrast with usual desktop systems where every user has a different UID and any application is being run under the users UID. Android uses permissions based security model for each application that runs on the system. Upon installation, each application is given its unique UID used to protect the data from being shared with other applications (for data sharing a special permission is required) and the application will always run with that UID on that particular device. Also, Android developers are required to sign their code, the main advantage of this being the possibility for the developers to update their code without special permissions (the applications signed with the same key – created by the same user – can run with the same UID). Although being an open source platform, Android is able to offer a high security level through its application development architecture, permissions model and application signing requirements [8].

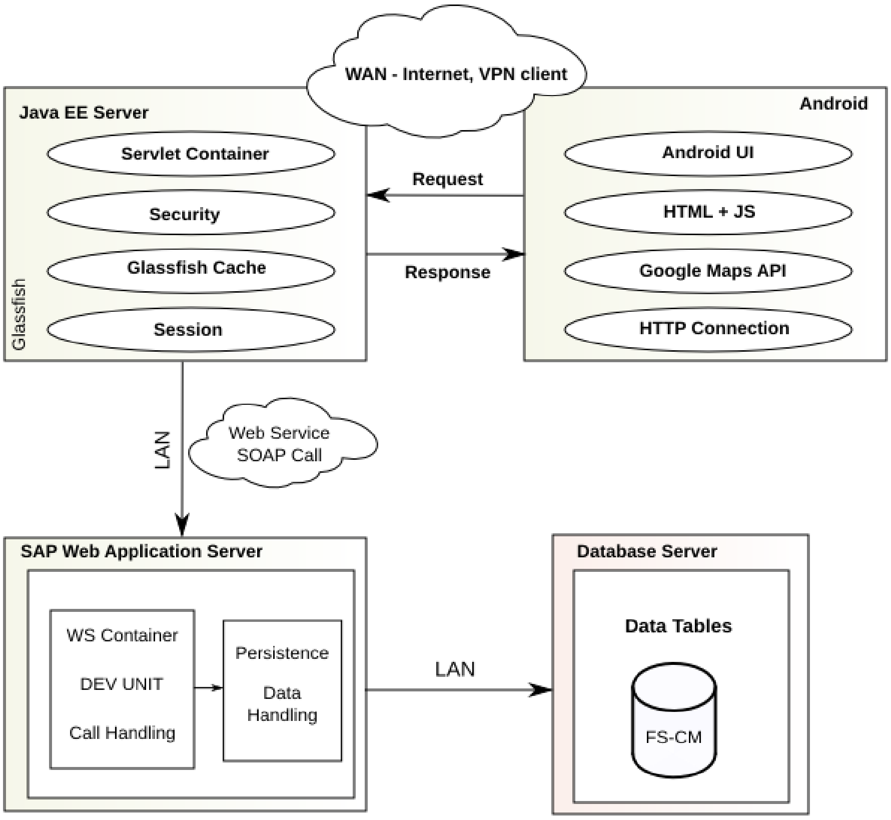

Fig. 3. Mobile application system overview

Security in the Glassfish application server and the J2EE environment is achieved through the Transport Level Security (TSL) and Secure Sockets Layer technologies, through a system of authentication and authorizations that grant access control permissions and through the use of Message Level Security in Web Services.

The SAP Web Application Server, the application server for SAP solutions has a five layers architecture: the presentation layer enables the development of the user interface with Java Server Pages (JSP), Business Server Pages (BSP) or Web Dynpro technology; the business layer consists of a J2EE runtime environment in which the business logic can be implemented in ABAP or Java programming language; the integration layer allows the exchange of messages between the components; the connectivity layer uses several communication protocols such HTTP, HTTPS, SMTP, SOAP and FastCGI; the database layer supports database independence, offers a wide range of APIs and ensures access through Open SQL for ABAP and Java. The security of the SAP WAS is ensured at different levels: the network and communication level, security for the ABAP technology, security for Java technology, security of the Internet Transaction Server, etc.

The security offered by the Mobile Inspector application is solely based on the security system of the technologies involved in the development and implementation, described above, plus an authentication through user and password on the mobile application itself. The mobile application resident on the device sends simple requests to the Java Web Server, where these request are interpreted and transmitted in form of Web Service further to the SAP Web Application Server. A response is sent from the SAP Web Server to the Java Server, and then forwarded to the mobile application.

2.3 The alternative: using SAP Mobile Infrastructure

SAP NetWeaver Mobile Infrastructure (SAP NetWeaver MI) is a technology solution of SAP NetWeaver used for the development of applications for mobile business processes (SAP solutions and other mobile applications not SAP-based). It consists of four main components: the Data Orchestration Engine, a thick client resident on the mobile device, a mobile administration and monitoring tool and NetWeaver Developer Studio. SAP MI is installed locally on a mobile device and it comes with a Web server, a database layer and its own business logic. This represents an advantage for the end-users as it enables the possibility of working offline remotely. SAP MI contains tools for synchronization and data replication, ensuring the consistency of the data on both mobile device and backend system. The Data Orchestration Engine enables the exchange of data between the back-end systems and the mobile devices, through a data consolidation, data realignment and data staging specially configured middleware server. The mobile client ensures a store and forwarding mechanism for connected scenarios. The overall mobile landscape is managed with the help of the administrative and monitoring tools.

SAP Mobile Infrastructure is an open standard-based platform (using Java, eXtensible Markup Language (XML) and Simple Object Access Protocol (SOAP)) that offers secure access to information and enables business processes. It also has a Java virtual machine and offers an open programming model on which mobile applications can be developed. This open platform architecture provides network and device independence, supporting a wide range of mobile devices (PDAs, laptop computers and smart phones) and various network types (wireless LANs, Bluetooth and GPRS) [7].

The SAP MI Architecture consists of three elements: the mobile device on which the mobile application is installed and used by the client, a SAP NetWeaver Application Server which controls and monitors the mobile infrastructure and is used for the communication and data exchange between the mobile application and the backend system, and several backend systems which are available to the server-side of the mobile application.

The Client Mobile Infrastructure provides the following services: UI programming model (through Java Server Pages or Abstract Window Toolkit) and framework services as Java APIs used for data synchronization, data persistence, data manipulation, logging and tracing, etc.

The server is part of the SAP NetWeaver Application Server and uses both the Java and the ABAP stack. As part of the Java stack, SAP MI J2EE Server Component has the task of passing the data containers from the SAP MI Client Component to the SAP MI ABAP Server Component and managing the mobile devices and components. The SAP MI ABAP Server Component of the ABAP stack is responsible for data replication, the queuing and acknowledgement of the synchronized data containers, for communicating with the backend system and for the deployment of mobile applications on the mobile device.

The backend system consists of customizing and repository objects that are transported to the frontend system using the standard mechanism of SAP Change and Transport System.

When it comes to evaluating the security level of a mobile system, one must take into consideration primarily the “mobility threat”: a mobile device is much more vulnerable than a server because it is usually handled in open space; it is relatively easy to access the file system of a mobile device and the operating systems do not provide sufficient protection against access nor authorization system for data manipulation at file level; also the number of users and the threat of loss of theft increase its vulnerability. Using the SAP Mobile Infrastructure for mobile applications development, on the other hand, has various advantages from the security point-of-view, such as the data synchronization and replication mechanism offered and the high security of the architecture model.

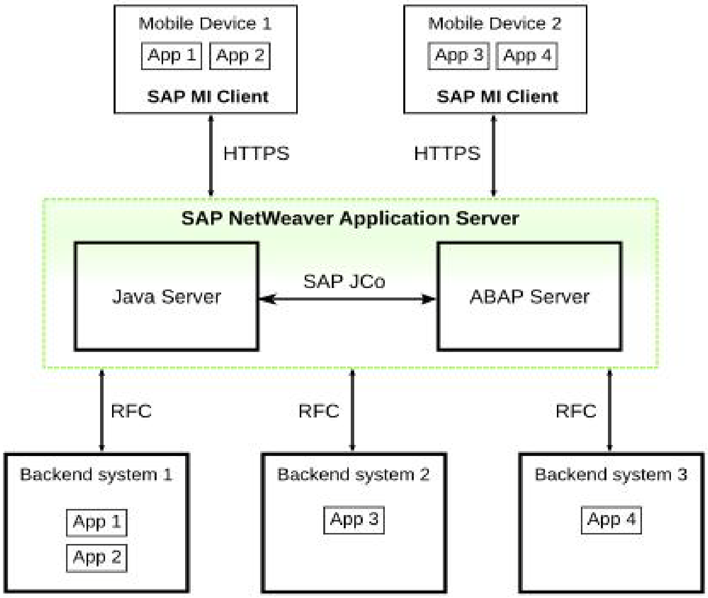

Fig. 4. SAP Mobile Infrastructure Architecture

Data synchronization and replication: the data is synchronized between the SAP MI application server and the mobile application in a two-way mode (from the server to the mobile application and vice-versa). The data is packed in special containers in XML format and transmitted in a compressed and coded form, as synchronization provides a secure, encrypted and compressed data transfer executed over the Hypertext Transfer Protocol with Secure Sockets Layer (HTTPS). Through the administration and monitoring tools of the SAP MI, the data replication process is ensured with a high level of security, the data packages are replicated according to their novelty (through delta comparison), and any conflict between the mobile device and the server application is detected and solved (conflict management).

Security of the infrastructure: the main security capabilities of SAP MI include authentication (user ID and password protection, X.509 digital certificates), role-based authorization, secure network connections via SSL, strong encryption and integrity protection, integrated management and Single-Sign-On (SSO).

3 Security aspects in SAP Mobile Infrastructure

The security of the mobile applications developed on the SAP NetWeaver Mobile Infrastructure is ensured in several stages: authentication and user administration level, authorization and role-based level, network and communication channel security and data security. The server uses the SAP User Administration function from the SAP Web Application Server (SAP Web AS) for authentication and user management purposes, as this can be performed through three distinct activities: authentication with user and password, authentication using system logon and authentication with Single-Sign-On.

User administration and authentication

Authentication with user and password: this type of authentication is provided in two steps: the authentication to the SAP MI Client Component that has its own user administration system (for the local user and local password) and to the SAP MI Server

Component through a synchronization password. For working offline, the user must authenticate himself to the system using the local password (stored in encrypted form on the mobile device), whereas for working online the authentication consists in the matching of the local password to the synchronization password on the server side.

Authentication using system logon: this type of authentication is predominantly used when the mobile device has a single user which can authenticate himself to the operating system, and therefore bypass the local password authentication step.

Authentication with Single-Sign-On: authentication with SSO can be used if the mobile device has a online connection. This type of authentication is based on the issuing of a logon ticket from a system (e.g. SAP Enterprise Portal) that the client can use further to authenticate himself to the server without requiring any other password.

Authorization – Roles

The role-based authorization in SAP MI ensures a high level of security for the mobile applications. The data and application access is controlled by a data-filtering system based on the SAP authorization concept. Under this concept one can create different types of roles (roles for users of the mobile applications, roles for system administrators, roles for service users for anonymous synchronization or administration purposes) and assign one or more authorization objects them.

Network and communication channels security

SAP MI uses Hypertext Transfer Protocol (HTTP) or Secure Hypertext Transmission Protocol (HTTPS) for communications between the mobile device and the server. The data is transferred only after the user is authenticated by the SAP MI Server Component using one of the above mentioned methods, through certain channels (wrapper functions, SyncBOs, synchronization between the SAP MI Client and Server Components).

For the communication between the mobile device and the server, the infrastructure is based on the following channels:

- from the SAP MI Client Component to the SAP MI J2EE Server Component and vice-versa using the HTTP, Secure Socket Layer (SSL) or HTTPS technology;
- from the SAP MI J2EE Server Component to the SAP MI ABAP Server Component and vice-versa through SAP Java Connector (SAP JCo);
- from the SAP MI ABAP Server Component to the backend system and vice-versa through Remote Function Call (RFC).

Application data can be exchanged between the SAP MI Client (the mobile device), the SAP MI Server and the backend system. The control data of the SAP Mobile Infrastructure is only exchanged between the mobile device and the SAP MI Server. Because of the importance of the data exchanged in the system, a special protection is required and ensured through a system of local – synchronization passwords. With each HTTP request the synchronization password is copied from the mobile device to the SAP MI J2EE Server Component and the use of HTTPS or SSL technology increase the security aspect of this communication channel. Subsequently, the synchronization password is copied from the SAP MI Java Server Component to the SAP MI ABAP Server Component through the SAP Java Connector with a Secure Network Communication (SNC).

SAP MI offers an advanced acknowledgement mechanism between SAP MI Client Component and SAP MI ABAP Server, based on individual acknowledgement information – successful delivery and processing - on both servers (after the sending of each data container an acknowledgement from the receiver is awaited; if no acknowledgement is received, the data is sent again; if the receiver already processed the data container but the sending of the acknowledgement failed, the processing is not executed and another acknowledgement is sent). Every data container is guaranteed to the successfully delivered and executed exactly once and also the data file containing all the data containers in ASCII format are compressed dynamically.

Communication Destinations

For the connection to the backend systems, SAP MI uses the Remote Function Call (RFC) protocol over SNC. The communication between the systems can be synchronous or asynchronous: for synchronous synchronization, the RFC destination is defined as using the same user and password as used on the server; in case of asynchronous synchronization, a batch user is responsible for the logon to the backend system.

Data security

The data stored on the SAP MI Client Component (the mobile device) is not actively protected as the one stored on the SAP MI ABAP Server. For this reason certain security measures should be considered when dealing with personal data on the mobile device: the encryption of the directory structure in which the data from the SAP MI Client Component is stored, the use of an antivirus program, the avoidance of installing applications from unknown sources, the protection of the access to the operating system through a PIN number, user and password.

4 Conclusions

Business process mobilization represents taking advantage of the IT infrastructure and the latest technology advances, especially in the communication area, and extending a company's processes within and beyond its boundaries. Using the advantages offered by the mobile technologies (fairly simple to handle and low cost mobile devices that offer instant access to information, applications and services beyond the bounds of time and space, offline functionalities, higher level of responsiveness and better decision-making and control of the business processes) raises a company's value above its competitors. In the insurance business, the work of the insurance inspectors is a rather complex and time-consuming one, since the assessment of loss in case of accident and the decision on the rightfulness of the required compensation amount has to be done on the scene. Mobile applications offer a solution to these crucial problems by reducing operational costs and increasing work efficiency.

When choosing the technologies for the development of a mobile application, cost and security are two of the most important decision factors. Building a mobile application on Android operating system aims to be more efficient cost-wise, mostly due to the open availability of the platform and to its cost-free implementation framework. Using on the server-side the SAP NetWeaver platform with an SAP database server raises the costs of this customized solution and makes this approach less-effective in comparison to using the integrated and higher priced development platform SAP Mobile Infrastructure. On the other hand, the security aspect is better represented in the later case, having a number of additional advantages: the platform architecture is device and network independent, supporting a wide range of mobile devices and network types; applications can run offline due to the disconnected framework that runs on the mobile device; information is highly monitored through a synchronization framework from the device through a middleware to the backend system, etc.

Building applications on an integrated development platform made available by SAP - the market and technology leader in the area of business management software – ensures full technical and professional support, a higher security level and confidence in the resulted product, therefore we conclude that choosing SAP Mobile Infrastructure is a better decision given the factors described in this paper.

Acknowledgement

This work was supported by ANCS-CNMP, project number PNII – 91049/2007

References

[1] H. Johansson, *Business Process Reengineering: Breakpoint Strategies for Market Dominance*, John Wiley & Sons, 1993

[2] L. Pajunen and A. Ruokonen, "Modeling

and Generating Mobile Business Processes," IEEE International Conference on Web Services (ICWS 2007), ICWS, pp. 920-927, 2007.

[3] A. Köhler and V. Gruhn, *Analysis of Mobile Business Processes for the Design of Mobile Information Systems*, 2004

[4] H. van der Heijden and P. Valiente, "Mobile Business Processes: Cases from Sweden and the Netherlands," Stockholm School of Economics, SSE/EFI Working Paper Series in Business Administration, 2002.

[5] S. Stephansen, *Service-Oriented Mobile Business Process Execution*, Available at: www.bptrends.com

[6] C. Ciumas, *Asigurari generale*, Casa Cartii de Stiinta, 2009.

[7] *Security Guide for SAP Mobile Infrastructure*, SAP Press, 2004

[8] J. Burns, *Mobile Application Security on Android*, Black Hat USA, 2009

[9] *SAP Application Server Security Guide*, SAP Press, 2004

Ilona-Mariana NAGY has a Bachelor's degree in Economic Informatics and a Master's degree in Economic Informatics and the Informational Society from the Faculty of Economics and Business Administration, Babeș-Bolyai University of Cluj-Napoca. Starting from 2009 she is a PhD student in Business Information Systems at the same educational institution, her main scientific fields of interest including: databases, data warehouses, business intelligence and SAP technologies.