CIM to PIM Transformation: A Reality

Alfonso Rodríguez[1], Eduardo Fernández-Medina[2] and Mario Piattini[2]

[1] Departamento de Auditoría e Informática,Universidad del Bio Bio,Chillán,Chile
alfonso@ubiobio.cl
[2] ALARCOS Research Group, Information Systems and Technologies Department, UCLM-Indra Research and Development Institute, University of Castilla-La Mancha, Ciudad Real, Spain {Eduardo.FdezMedina,Mario.Piattini}@uclm.es

Abstract. Within the scope of MDA, the model transformation is orientated towards solving the problems of time, cost and quality associated with software creation. Moreover, business process modeling, through the use of industrial standards such as UML or BPMN, offers us a good opportunity to incorporate requirements at high levels of abstraction. We consider Secure Business Process models such as the Computation Independent Model (CIM). In this paper we show that it is possible to define CIM to PIM (Platform Independent Model) transformations, using QVT rules. Through our rules, we obtain certain UML analysis-level classes and use cases which will be part of the PIM of an information system. We illustrate our approach with a case study concerned with payment for the consumption of electrical energy.

Keywords: *Business process, MDA, Requirement specifications, Security*

1. INTRODUCTION

Software engineering is currently greatly influenced by MDA, a new paradigm which claims to work both at a model and at a metamodel level. The MDA approach is not based on one single idea. Among the objectives pursued, are the separation of business-neutral descriptions and platform dependent implementations, the expression of specific aspects of a system under development with specialized domain-specific languages, the establishment of precise relations between these different languages within a global framework and, in particular, the capability of expressing operational transformations between them [1]. The MDA approach is composed of: the Computation Independent Model (CIM), the Platform Independent Model (PIM), and the Platform Specific Model (PSM) [2].

Because these models represent a different abstraction of the same system, an integration/transformation mechanism is required to establish *how* to go from one level (e.g. CIM) to another (e.g. PIM). Thus, transformations are a core element in the MDA. In the last few years, the most ambitious bet is QVT (Query/View/Transformation) [3], the transformation language proposed by the OMG. QVT plays an important role in the OMG metamodel family, because it includes special features which can be used to perform transformations within these frameworks.

On the other hand, enterprise performance has been linked to the capacity which each of these enterprises has to adapt itself to the changes that arise in the market. In this context, Business Processes (BP), defined as a set of procedures or activities which collectively pursue a business objective or policy goal [4], have become valuable resources that have been used to maintain competitiveness.

Although the importance of business process security is widely accepted, until now the business analyst perspective in relation to security has hardly been dealt with. In [5, 6] we introduced security representation into business processes. To do so, we extended the UML 2.0 Activity Diagram (UML 2.0-AD) [7] and the Business Process Modeling Notation - Business Process Diagram (BPMN-BPD) [8]. A BPSec profile was created which allows us to the capture security requirements expressed by the business analyst. Such a specification gives origin to a Secure Business Process.

A business process built by a business analyst is not only useful in the specific business field but is also very useful in a process of software construction, and can be used to obtain system requirements, a stage taken into account by all modern development processes.

In this paper, we demonstrate how a set of analysis-level classes and use cases, both considered as being a PIM, can be obtained from the specification of a Secure Business Process, which is considered to be a CIM. The transformations have been described as a set of QVT rules and refinement rules. All of the artifacts, the Secure Business Process, the Analysis-level class, and the Use case, can be used in the software development process.

The structure of the remainder of the paper is as follows: in Section 2, we shall summarize the main backgrounds which explain the method that we have designed in order to incorporate security into business processes, the various steps of which they are made up and the tool which supports the realization of these stages. Finally, in Section 3, we will describe a case study and in Section 4 our conclusions will be drawn.

2. BACKGROUND

The main works related to security requirements specification in business processes [9-13] all coincide in the idea that it is necessary to capture the point of view of the business expert with regard to security, and to include these specifications within the software development process.

At present, security requirements which are easily identifiable by those who model business processes can be captured at a high level because: (i) business process representation has improved in UML 2.0-AD and BPMN-BPD, (ii) the security requirement tends to have the same basic kinds of valuable and potentially vulnerable assets [14], and (iii) empirical studies show that it is common at the business process level for customers and end users to be able to express their security needs [15].

Consequently, we have approached the problem of including security in business processes by extending the BPMN-BPD [6] and UML 2.0-AD [5] which allows business analysts to specify security requirements. The proposed extension, which we have called BPSec-Profile, considers the graphical representation of security requirements; a non-limited list, taken from the taxonomy proposed in [14].

In our proposal we have used a padlock, standard *de facto*, to represent security requirements. The same symbol, the padlock, but with a twisted corner is used to represent a Security Requirement with Audit Register (see Figure 1).

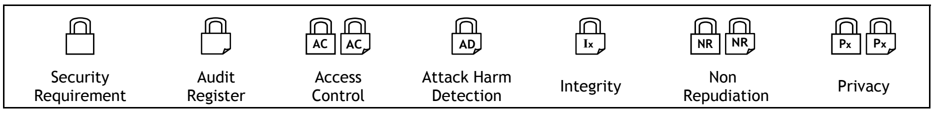

Figure 1. Icons used in BPSec

As a result of the application of the BPSec-Profile, a Secure Business Process (SBP) is obtained. This description is used to obtain the analysis-level classes and use case in which security forms a part of the diagrams obtained.

In this paper, CIM to PIM transformations are aimed at obtaining useful artifacts in software development. The basic aspects of our proposal are shown in Figure 1. The first column (on the left) shows two types of models which conform to the MDA. In the last column we can see the Unified Process [16] disciplines. The central part shows our proposal and the artifacts which are derived from its application. The business process specification is made by using UML 2.0-AD and BPSec-Profile. We applied a set of QVT rules, refinement rules and checklists to obtain a subset of analysis-level classes and use cases that facilitate the understanding of the problem. SBP is used in "Business Modeling" and use cases are used in the "Requirement" and "Analysis & Design" disciplines of the Unified Process.

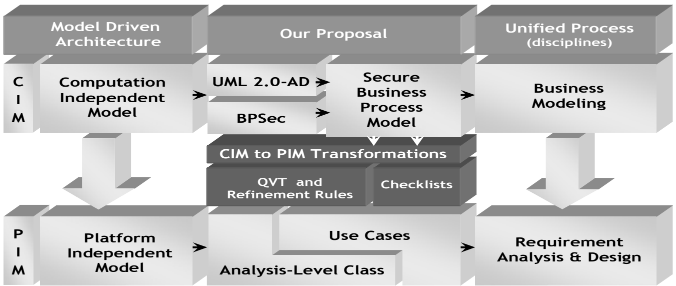
Model Driven Architecture
Our Proposal
Unified Process (disciplines)
C I M
Computation Independent Model
UML 2.0-AD
BPSec
Secure Business Process Model
Business Modeling
CIM to PIM Transformations
QVT and Refinement Rules
Checklists
P I M
Platform Independent Model
Use Cases
Analysis-Level Class
Requirement Analysis & Design

Figure 2. An Overview of Our Proposal

In order to apply the BPSec-profile and to obtain artefacts which will be useful in a software development process, we have designed a method called M-BPSec [17] (see Figure 3). This method permits the ordered and systematic carrying out of the elicitation of security requests and the attainment of analysis cases and use cases. M-BPSec considers stages, workers, tools, models and artifacts which, if grouped together, permit (i) the design of an SBP (ii) the attainment of analysis-level classes and use cases which include security aspects and (iii) the storage of information related to the specification of the business process.

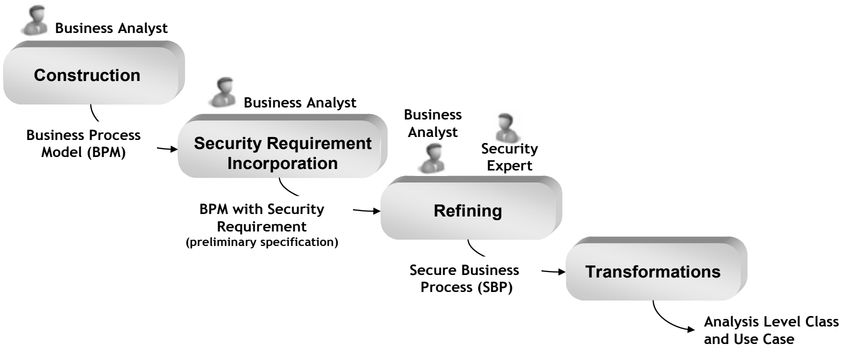
Business Analyst
Construction
Business Process Model (BPM)
Business Analyst
Security Requirement Incorporation
BPM with Security Requirement (preliminary specification)
Business Analyst
Security Expert
Refining
Secure Business Process (SBP)
Transformations
Analysis Level Class and Use Case

Figure 3. M-BPSec Overview

Each of the stages of M-BPSec is technologically supported by the BPSec-Tool (see Figure 4). This tool is used to design the SBP, to automatically transform models and to update the data contained in the secure business process repository. The BPSec-Tool was built by using a 3-tiered architecture to separate the presentation, application, and storage components, using MS-Visio, C#, and MS-Access technology respectively.

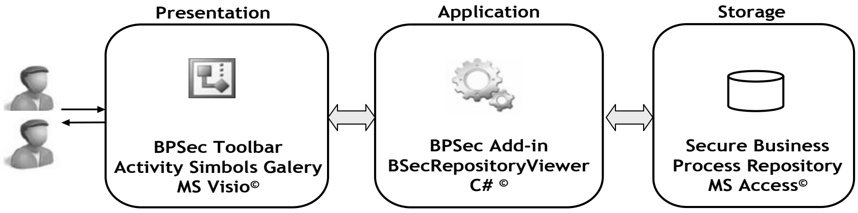

Figure 4. The Components of the BPSec-Tool

The transformations from the secure business process to the analysis clases are carried out by using a set of QVT rules and Refinement rules, a detailed description of which can be found in [18]. Basically, an equivalence relationship is established between the elements in both metamodels. A subset of the QVT rules is shown in Table.

The transformations from the secure business process to the use case are carried out by using a set of QVT rules, Refinement rules and a Checklist a detailed description of which are given in [19]. As with the analysis classes, the QVT rules permit the unidirectional transformation of the elements in both metamodels. A subset of the QVT rules is shown in Table. The checklists are used to obtain use cases related to the security specifications.

In both cases, the Refinement rules are applied after the QVT rules. The objective of this is to enrich both the analysis classes and the use cases by incorporating significant names, identifying relationships between classes and establishing dependencies between actors.

Table 1. Mapping from UML 2.0-AD/BPSec-Profile to Analysis-level Classes and Use Cases

```
transformation ActivityDiagram2ClassDiagram
  top relation R1  // from Activity Partition to Analysis-Level Class
  {
    checkonly domain uml_ActivityDiagram ap:ActivityPartition {name = n}
    enforce domain uml_ClassDiagram c:Class {name = n}
    where { ap.containedNode → forAll(cn:Action|R4(cn))}
  }
  top relation R2  // from Interruptible Activity Region to Analysis-Level Class
  {
    checkonly domain uml_ActivityDiagram iar:InterruptibleActivityRegion {name = n}
    enforce domain uml_ClassDiagram c:Class {name = n}
    where { ap.containedNode → forAll(cn:Action|R4(cn))}
  }
  top relation R3  // from Data Store Node to Analysis-Level Class
  {
    checkonly domain uml_ActivityDiagram dsn:DataStoreNode {name = n}
    enforce domain uml_ClassDiagram c:Class {name = n}
  }
  relation R4 // from Action to Operation in Analysis-Level Class
  {
    checkonly domain uml_ActivityDiagram ac:Action {name = n, inPartition=ap}
    enforce domain uml_ClassDiagram op:Operation {name = n, ownerClass=c:Class{name=ap.name}}
  }
transformation ActivityDiagram2UseCaseDiagram
  top relation R1  // from Activity Partition to Actor
  {
    checkonly domain uml_ActivityDiagram ap:ActivityPartition {name = n}
    enforce domain uml_UseCaseDiagram a:Actor{name = n}
    where {
         ap.containedNode → forAll(cn:Action|R3(cn))
    }
  }
  top relation R2  // from Interruptible Activity Region to Actor
  {
    checkonly domain uml_ActivityDiagram iar:InterruptibleActivityRegion {name = n}
    enforce domain uml_UseCaseDiagram a:Actor {name = n}
    where { ap.containedNode → forAll(cn:Action|R3(cn))
    }
  }
  relation R3 // from Action to UseCase
  {
    checkonly domain uml_ActivityDiagram ac:Action {name = n, inPartition=ap}
    enforce domain uml_UseCaseDiagram uc:UseCase {name = n, subject= ACTORS: Set(Actor)};
    where { ACTORS→including (a:Actor{name=ap.name})
    }
  }
transformation BPSec2UseCaseDiagram
  top relation R1  // from Security Requirement to subject
  {
    checkonly domain bpsec_BPSec sr:SecurityRequirement {requirementtype = n}
    enforce domain uml_UseCaseDiagram c:Clasifier {name=n}
  }
  top relation R2  // from Security Requirement to subject
  {
    checkonly domain bpsec_BPSec sr:SecurityRequirement
    enforce domain uml_UseCaseDiagram a:Actor {name="Security Staff"}
  }
```

In the following section, we have developed a case study through which to show the CIM to PIM transformations. This is done by using the M-BPSec method which is supported by the BPSec-Tool.

3. A CASE STUDY

The case study has been developed in a cooperative which is dedicated to the distribution of electricity in rural areas. The Coopelan Ltda. (www.coopelan.cl) cooperative came into being in 1957, and currently maintains 2,200 kms of electrical lines which are used to supply more than 12,000 clients. Recent years have seen the commercialization of goods and services, both for their clients for electrical energy (who are associates of the cooperative) and for the public in general. From an organizational point of view, the cooperative is made up of a technical area which is related to the distribution of electricity, a commercial area which is in charge of goods and services, and an administrative area. The cooperative has a total of 70 employees.

Because the cooperative's main clients live in rural areas, the way in which they presently receive payment for the consumption of electricity presents two problems: (i) delivery of the invoice upon which the consumption of electrical energy is detailed and (ii) receipt of payment of said debt. Business analysts have used a traditional method to modify the business process associated with the recovery of energy consumption debts, and have incorporated an electronic debt advisor and electronic payment. This complementary method has increased the index of debt recovery. The cooperative has neither the technical nor the operative capacity through which to receive electronic payments (via the Internet) and for this reason it has decided to employ an external collector to carry out this task.

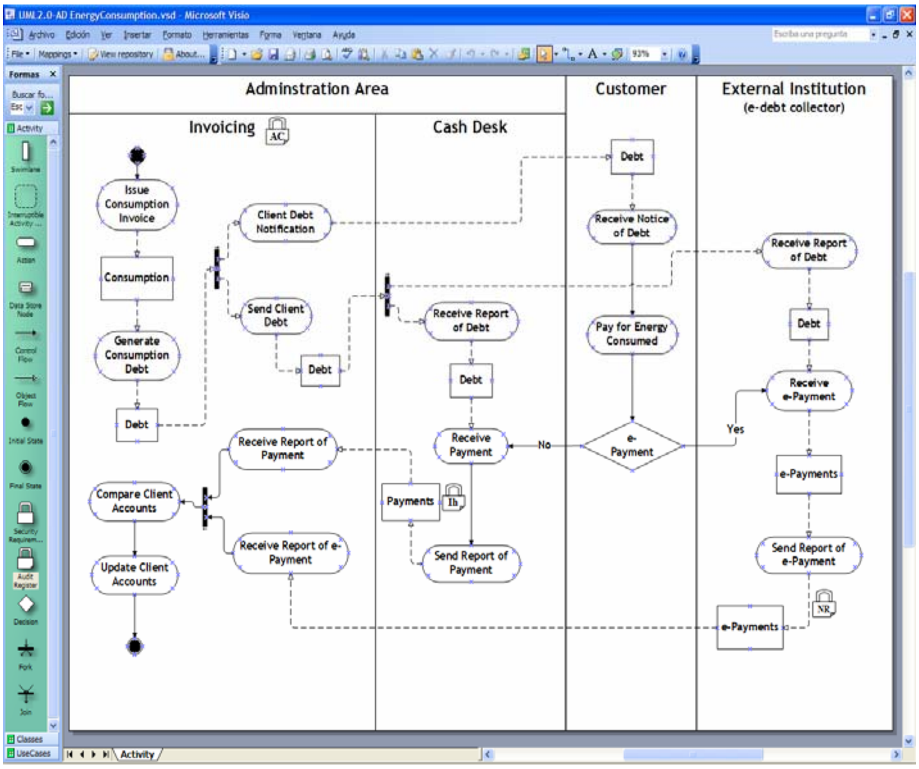

Figure 5. Secure Business Process: Payment for Consumption of Electrical Energy

The business process which we shall describe as a part of our case study is about payment for consumption of electrical energy. The case study was carried out with the assistance of the cooperative's business analysts. M-BPSec was used in the development of this case study. The result of the first three stages is a Secure Business Process called "*Payment for consumption of Electrical Energy*", which is shown in Figure 5.

Details of the application of the stages of M-BPSec are:

- The *Construction* stage basically consists of producing a business process, and this is done by the business analyst. In this case, the business process was described by using the UML 2.0-AD. The areas which were identified were Activity Partitions "External Institution", "Customer", and "Administration Area", which was divided into two central Activity Partitions called "Invoicing" and "Cash Desk". This business process is initiated when the "Issue Consumption Invoicing" activity is carried out, and it terminates with receipt of payments and an updating of clients' debts.
- In the *Security Requirement Incorporation* stage, the business analyst identifies which, from his/her point of view, are the vulnerable areas in the business process. A meeting has previously taken place in which the significance of the security requirements considered in the BPSec-Profile is explained. The business analyst identifies vulnerable areas in: (i) the information which is sent from "External collector" to "Invoicing", for which Non-repudiation is specified, (ii) the information related to the payments received in the "Cash Desk", for which a high level of Integrity is specified, and (iii) the activities and information related to the Invoicing Activity Partition for which Access Control is specified
- The *Refinement* stage was carried out by the business analyst in conjunction with the security expert. These people analyzed and agreed upon the security requirement specifications and added Audit Register to the Non-Repudiation and Access Control specifications.
- Finally, the *Transformations* stage was applied to the secure business process. This stage was carried out automatically by using the BPSec-Tool. The results obtained were the analysis class diagram shown in Figure 6 and the Integrity in payments and Non repudiation for message use cases (see Figure 7), general use case for payments for consumption of electrical energy and access control in invoicing (see Figure 8).

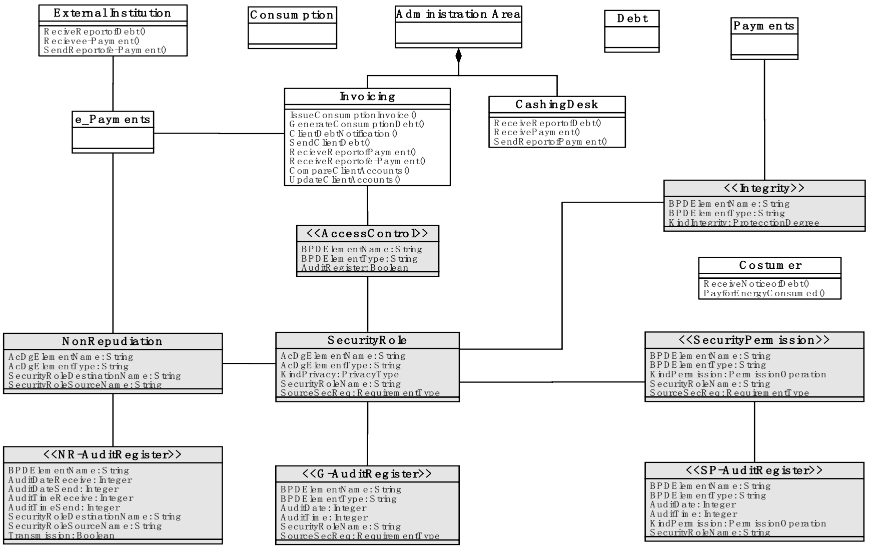

Figure 6. Class Diagram from "Payment for Consumption of Electrical Energy

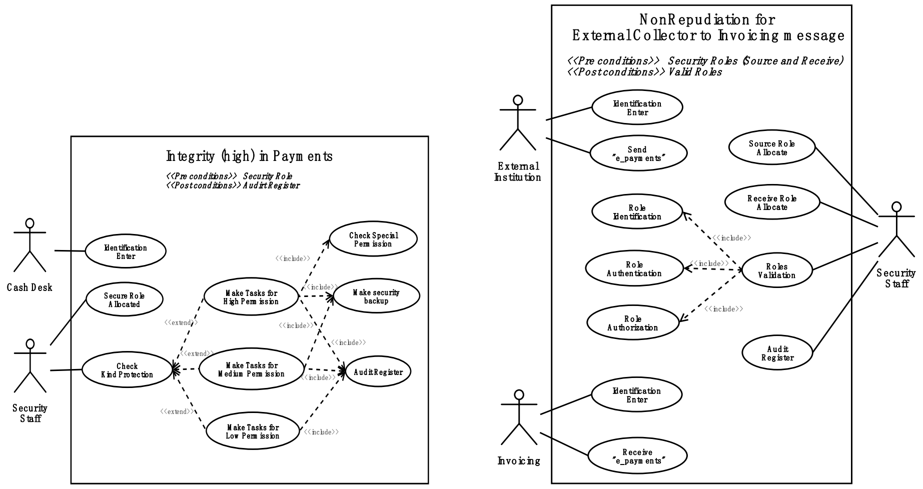

Figure 7: *Integrity* and *NonRepudiation* Security Use Cases Specification

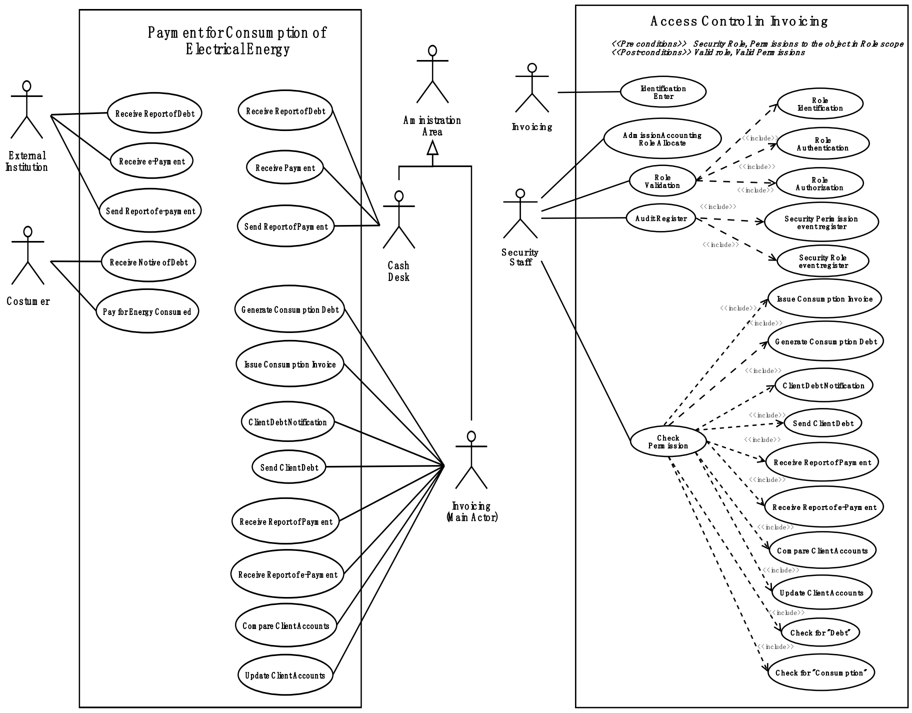

Figure 8. *General a*nd *Access* Control Use Cases Specification

Both the secure business process and the analysis classes and use cases have been used as input in the software development process which Coopelan Ltda. used to carry out its software creation.

4. CONCLUSIONS

A business process specified with a UML 2.0 Activity Diagram containing security requirement allows the incorporation of a new perspective with regard to the security in a software creation process.

In this paper, we have used a case study to show that it is possible to make transformations from Computational Independent Models to Platform Independent Models (CIM to PIM). In addition, both the Secure Business Process and the Analysis-level Classes and Use Cases can be used in a software construction process.

The next steps in our research are orientated towards applying our proposal to projects of a greater scope, with the intention of enriching the method and improving the transformations in order to obtain more complete class models and use cases. Additionally, we shall also improve the BPSec-Tool in order to allow us to include other notations for the specification of the Secure Business Process.

ACKNOWLEDGEMENTS

Thanks to Mr. Eduardo Robba, business and system analyst of Coopelan Ltda., by its valuable collaboration in the development of the case study. This research is part of the following projects: DIMENSIONS (PBC-05-012-1), and MISTICO (PBC06-0082) both partiality supported by the FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", Spain, COMPETISOFT (506AC087), granted by CYTED and ESFINGE (TIN2006-15175-C05-05/) granted by the "Dirección General de Investigación del Ministerio de Ciencia y Tecnología", Spain.

REFERENCES

1. J. Bézivin, In Search of a Basic Principle for Model Driven Engineering, *UPGRADE, European Journal for the Informatics Professional.* Volume 5, Number 2, pp.21-24, (2004).
2. Object Management Group, *MDA Guide Version 1.0.1.* http://www.omg.org/docs/omg/03-06-01.pdf. (Accessed 2003).
3. QVT, *Meta Object Facility (MOF) 2.0 Query/View/Transformation Specification*, OMG Adopted Specification ptc/05-11-01 (2005), p.204.
4. WfMC, *Workflow Management Coalition: Terminology & Glossary* (1999), p.65.
5. A. Rodríguez, E. Fernández-Medina, and M. Piattini, Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes, in *Proc. of 3rd International Conference on Trust, Privacy and Security in Digital Business (TrustBus). Volume 4083* (Krakow, Poland, 2006), pp.51-61.
6. A. Rodríguez, E. Fernández-Medina, and M. Piattini, A BPMN Extension for the Modeling of Security Requirements in Business Processes, *IEICE Transactions on Information and Systems.* Volume E90-D, Number 4, pp.745-752, (2007).
7. Object Management Group, *Unified Modeling Language: Superstructure Version 2.1.1 (formal/2007-02-05).* http://www.omg.org/docs/formal/07-02-05.pdf (Accessed 2007).
8. BPMN, *Business Process Modeling Notation Specification*, OMG Final Adopted Specification, dtc/06-02-01. http://www.bpmn.org/Documents/OMG%20-Final%20Adopted%20BPMN%201-0%20Spec%2006-02-01.pdf (Accessed 2006).
9. M. Backes, B. Pfitzmann, and M. Waider, Security in Business Process Engineering, in *International Conference on Business Process Management (BPM). Volume. 2678, LNCS* (Eindhoven, Netherlands, 2003), pp.168-183.
10. G. Herrmann and G. Pernul, Viewing Business Process Security from Different Perspectives, in *Proc. of 11th International Bled Electronic Commerce Conference* (Slovenia, 1998), pp.89-103.
11. P. Herrmann and G. Herrmann, Security requirement analysis of business processes, *Electronic Commerce Research.* Volume 6, Number 3-4, pp.305-335, (2006).
12. A. Maña, J. A. Montenegro, C. Rudolph and J. L. Vivas, A business process-driven approach to security engineering, in *14th. International Workshop on Database and Expert Systems Applications (DEXA)* (Prague, Czech Republic, 2003), pp.477-481.

13. A. W. Röhm, G. Pernul and G. Herrmann, Modelling Secure and Fair Electronic Commerce, in *Proc. of 14th. Annual Computer Security Applications Conference* (Scottsdale, Arizona, 1998), pp.155-164.

14. D. Firesmith, Specifying Reusable Security Requirements, *Journal of Object Technology.* Volume 3, Number 1, pp.61-75, (2004).

15. J. Lopez, J.A. Montenegro, J.L. Vivas, E. Okamoto and E. Dawson, Specification and design of advanced authentication and authorization services, *Computer Standards & Interfaces.* Volume 27, Number 5, pp.467-478, (2005).

16. I. Jacobson, G. Booch and J. Rumbaugh, *The Unified Software Development Process* (1999), pp.463-.

17. A. Rodríguez, E. Fernández-Medina and M. Piattini, *M-BPSec: A Method for Security Requirement Elicitation from a UML 2.0 Business Process Specification*, in *3rd International Workshop on Foundations and Practices of UML* (Auckland, New Zealand, 2007).

18. A. Rodríguez, E. Fernández-Medina and M. Piattini, Analysis-Level Classes from Secure Business Processes through Models Transformations, in *Proc. of 4th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)* (Regensburg, Germany, 2007).

19. A. Rodríguez and I. García-Rodríguez de Guzmán, *Obtaining Use Cases and Security Use Cases from Secure Business Process through the MDA Approach*, in *Workshop on Security in Information Systems (WOSIS)* (Funchal, Madeira - Portugal, 2007).