J. Lopez, et al., "Specification and Design of Advanced Authentication and Authorization Services", *Computer Standards & Interfaces*, vol. 27, pp. 467-478, 2005.
http://doi.org/10.1016/j.csi.2005.01.005
NICS Lab. Publications: https://www.nics.uma.es/publications

Specification and Design of Advanced Authentication and Authorization Services

Javier Lopez [a] Jose A. Montenegro [a] Jose L. Vivas [a]

[a] *Computer Science Department, University of Malaga, Spain*

Eiji Okamoto [b]

[b] *Institute of Information Sciences and Electronics. University of Tsukuba, Japan*

Ed Dawson [c]

[c] *Information Security Research Centre. Queensland Univ. of Technology, Australia*

Abstract

A challenging task in security engineering concerns the specification and integration of security with other requirements at the top level of requirements engineering. Empirical studies show that it is common at the business process level that customers and end users are able to express their security needs. Among the security needs of Internet applications, authentication and authorization services are outstanding and, sometimes, privacy becomes a parallel requirement. In this paper, we introduce a methodology for the specification of security requirements and use a case of studies to apply our solution. We further detail the resulting system after extending it with an Authentication and Authorization Infrastructure.

Key words: Information Security, X.509 Certificates, Authentication, PKI, PMI, Authorization, Privacy, Business Process Model

1 Introduction

The evolution of Information Systems during the last years has brought a parallel evolution of Information Security. At the same time, the importance

Email addresses: jlm@lcc.uma.es (Javier Lopez), monte@lcc.uma.es (Jose A. Montenegro), vivas@lcc.uma.es (Jose L. Vivas), okamoto@is.tsukuba.ac.jp (Eiji Okamoto), e.dawson@qut.edu.au (Ed Dawson).

of anticipating the impact of technical changes yet to come has increased dramatically.

One of the main objectives of Information Security is to optimize the performance of an organization with respect to the risks to which it is exposed. Standardization bodies have recognized the importance of Information Security. In this sense, ISO has recently published the *Code of Practice for Information Security Management* [1]. The document shows clearly the importance of information as business assets: "Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected." And, therefore, the necessity of Information Security: "Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities."

Security requirements and controls should reflect the business value of the information assets involved, as well as the potential business damage which might result from a failure or absence of security. The framework for the analysis of those security requirements and the identification of controls to fulfil originate important concepts as *risk assessment* and *risk management*.

Several governments, with the collaborations of private institutions, have developed surveys about the actual status of Information Security and its influence in the business scenario. For instance, the ninth edition of CSI/FBI Survey 2004 [2] has been designed to further explore a number of issues related to budgeting and financial management of information security risk. The survey presents the security technologies used in 2004. It is important to underline the inclusion of PKI technologies, in comparison with the 2003 survey, what demonstrate that advanced security technologies are being included in the business scenario.

Security actions can be classified as proactive or reactive. Proactive means that implemented security changes when a risk has been identified or demonstrated. Reactive means that implemented security changes forced by law or regulation, or only after suffering a security breach. Several security surveys show that most of corporations adopt a proactive approach. Thus, although the importance of the information security increases, the application of security technology is mostly applied when the software has been implemented.

A clear example of proactive application is a software patch. It is obvious that the intrusion rate increases constantly until the vulnerability is openly known and a patch is released. The expenses associated to this are normally very high. What is worst, a recent study shows that over 90% of the security exploits are carried out through vulnerabilities for which there are known patches.

On the other hand, the report [4] has studied the economic impacts of inade-

quate infrastructure for software testing, detailing the trends of the allocation of effort from 60s to 90s. In the study, two phases are clearly differentiated, pre-development and post-development. The pre-development phase consist of Design and Coding. The post-development phase consist of Internal Testing, Beta Testing and Post-Release. The report shows that 80% of the bugs are produced in the post development phases, and that cost associated to fix a bug in this phase differs between $10,000 and $30,000, whereas fixing a bug in pre-development phases is estimated between $1,000 and $5,000. Moreover, other surveys show that companies are spending a huge amount of money when trying to add security to final products. These issues clearly justify the need of including more effort in the pre-development phases, where fixing the bugs is cheaper.

This paper presents a business process-driven system development where technology decisions are guided by the business model. This model extends UML in order to express security notions in early phases of software development. In addition, an advanced authentication and authorization X.509-based solution is presented and, finally, a case study is used to apply the proposed methodology to authentication and authorization services.

The structure of the rest of this paper is the following. Section 2 discusses the relation between process modelling and security. Section 3 gives a brief overview of X.509 certificates, a standard solution to Authorization and Authentication. Section 4 presents our methodology, making use of a case study, the PASEN application, for a better understanding. Finally, section 5 concludes the paper.

2 Security Services Formalization

Although security aspects are inherent to any modern software systems, there is very little systematic support for software engineers to produce secure software. Conventional requirements modelling cannot represent the organisational procedures that underpin a security policy, and security policies are generally specified in terms of highly specialized security models that are not integrated with general software engineering models. However, there is currently agreement among experts that security engineering must be treated as an integral part of the overall system development process, and that computer systems security must address not just the computer system, but the changing organizational context in which they are inserted. A security implementation that ignores the basic phases of systems engineering: requirements, analysis, design, implementation, maintenance - is bound to fail.

It is necessary to use a business process-driven system development method

where technology decisions are guided by the business model. The concept of business process is of paramount importance in modern information technology. Business processes have been usually regarded as the starting point for system development, providing a simplified view of business structure and the system requirements necessary to support the business. Today we may regard them also as the endpoint of system development, its final product. With the advent of service-oriented architectures, information systems are now intended not primarily as a support to the business processes of an enterprise, but as business process in themselves at a cross-organizational basis. Business process security becomes thus a crucial aspect of modern information technology, since systems will only be deployed if enough assurances are given regarding its security properties.

On the other hand, capturing the security requirements of a system is a hard task that must be established at the initial stages of system development, and business spruces offer a view of business structure that is very suitable as a basis for the elicitation and specification of security requirements. Business process representations may in this way present in all stages of system development at different levels of abstraction appropriate for each stage.

If security semantics are encoded in each of these representations, this will greatly facilitate the task of traceability of security properties along different levels of abstraction, enable system developers to check for correctness of the security measures applied, and support the use of formal methods for the validation and verification of security properties at every stage of development. This will greatly enhance the prospects for compliance with the higher levels of assurance requirements established by the Common Criteria for Information Technology Security Evaluation [5], a standard of security evaluation for information technologies establishing *functional security requirements* (requirements on the product) and *security assurance requirements* (requirements on the process). Focusing on business process security requirements in the way we propose yields an encompassing process model for security engineering targeting both types of requirements.

The most challenging task in security engineering seems to be at the top level of requirements engineering. A dramatic example is given by the failure of the Pentagon's OSD [1] network. During deployment of the OSD network, an emergency was declared after an attempt to implement a security design to meet a very strict set of security policies. The cause was declared to be that the needs and requirements of both the users and the decision makers were not properly integrated into the security design and implementation. The original security components were basically correct and well-designed. The implementation of the security policies to be enforced by the security

[1] Office of the Secretary of Defense

hardware is where the system failure occurred. The system was re-engineered via an intensive effort to determine user and system data and communication requirements.

Security needs are typically articulated only as high level declarations by users and customers, corresponding to the business view of the system. Security concepts such as anonymity and privacy are part of the business view of security, whereas notions such as encryption or digital signature belongs to the technical view of security. It is also at the most abstract level that customers and end users are able to express their security needs. Empirical studies show that some form of business process review generally occurs among engineers and stakeholders in order to develop a common understanding on the security needs of a system. A formalization of this activity is thus called for.

With the aim of facilitating its adoption by system developers, we propose to integrate security requirements into standard system development methodologies, which currently is often use case-driven. Use cases are associated with the notion of scenario and sequence diagrams, whereas business process are based on workflow models and activity diagrams. However, at the most abstract levels of system specification these two kinds of diagrams are closely related, and one may be derived from the other in a variety of ways.

Modelling business surroundings involves answering the following questions: (i) how do different actors interact; (ii) what activities are part of their work; (iii) what are the ultimate goals of their work; (iv) what other people, systems or resources are involved that do not show up as actors to this specific system; and (v) what rules governs their activities and structures. The answers to these questions are important for the security aspects of a system.

The methodology we propose is consistent with the principles of the Model Driven Architecture (MDA) [6], a standard approach to model-driven development. MDA features three kinds of model: (i) *CIM*: Computer Independent Model (business model); (ii) *PIM*: Platform Independent Model (specification model); (iii) *PSM*: Platform Specific Model (implementation model). Business models (CIMs) are models of real-world objects and their behaviour.

In a business model, we include only the interfaces of the software systems, i.e. the services they provide. The requirements for the system are modelled in a computation independent model. A CIM is a model of a system that shows the system in an environment in which it will operate, and thus it helps in presenting exactly what the system is expected to do. It is useful both as an aid in understanding a problem and as a source of a shared vocabulary for use in other models. CIM requirements should be traceable to PIM and PSM constructs that implement them, and vice versa.

There are currently no general agreement about standards in the area of busi-

ness processes. Many candidate standards have been proposed, and many are under development. The area is in a state of turmoil, and it is an open question what the result of these standardizations efforts will be, even in the short run.

Two notational standards that have attracted most attention lately are the BPML (Business Management Language) [7] and BPEL4WS (Business process Execution Language for Web Services) [8]. The latter aims at actual execution of business processes using web service technology, and it is the business process notation that currently has the strongest support in industry. Other important business process standards are BPSS (Business Process Specification Schema) and XPDL (XML processing Description Language) [9]. All proposed standards are however XML-based. The Object Management Group has also recently become engaged in standardization work in business processes, and is working on initiatives towards the development of a standard meta-model for business processes. However, currently the notation with the strongest support is BPEL4WS.

Several formalisms have been used for giving a formal semantics to business process. Two of the most important are e.g. ConGolog [10] and Petri nets [11]. Petri nets are endowed with an operational semantics, graphical notations and executable techniques for specification, analysis and design of systems. They have been widely used in commercial software development and are well supported by formal specification tools. In Petri nets security may be defined in terms of reachability.

ConGolog is a concurrent logic programming language based on the situation calculus. A formalism based on first-order logic is suitable for the specification of a system at a high level of abstraction, as well as for reasoning, testing, validation and verification. With regard to business processes, it has been shown that they can be specified, synthesized, simulated, and tested for feasibility and consistency using ConGolog.

The basic concepts of this approach are *action, process, role, actor* and *goal*. The notions of actors and roles connect the process to the organizational model. Actions within a process are carried out in the context of an organizational role by actors. An action is defined by a set of preconditions and effects. A process is a first-order term of the language, a complex action which may take part in any kind of relation with e.g. goals, roles, resources, and other processes. A business process is defined as a network of actions performed in the context of organizational roles in pursuit of a set of goals. A process consists of a list of goals and a list of role definitions, and a role consists of a list of goals and a list of procedures for achieving these goals.

3 Advanced Authentication and Authorization Services

Public key certificates and *Public Key Infrastructures* (PKIs) [14] have brought to a new dimension the problem of *Authentication* and *Authorization*. A public key certificate (a.k.a. *digital certificate*, or *identity certificate*) is a data structure that represents an owners public key (and other optional information), verified and signed by a trusted authority in an unforgeable format. On the other hand, a PKI can be seen as a process for issuing digital certificates, which includes standards, authorities that issue certificates, communication between authorities and protocols for managing certification processes.

Digital certificates and PKIs can be used to provide an authentication infrastructure. Combined with some complementary technologies (e.g., attribute certificates), they can also be used as a starting-point to provide an authorization infrastructure.

An Authorization system needs to manage authorization information, and the management of this type of complex information additionally requires most of the times a solution that provides authentication, privacy, integrity and non-repudiation services. Different solutions make use of data objects with different data formats to carry the authorization information, like tokens, web cookies or identity certificates. We believe they present several drawbacks, either because these are not standard solutions or because they do not represent authorization information appropriately.

Commercial solutions present their own data structure format, like tokens or cookies, to store authorization information. Normally, proprietary formats present numerous bugs that produce security flaws in the whole system.

On the other hand, an X.509v3 public key certificate, standardized by ITU-T [15] can convey authorization information about its owner. The information is encoded in one of the X.509v3 extension fields, but there are several reasons that do not make this a convenient solution [16].

Instead of public key certificates, *attribute certificates* present a more suitable solution. An attribute certificate is a data structure that binds some attribute values with identification information about its holder. Meanwhile, this type of certificate has been incorporated into both the ANSI X9.57 standard and the X.509-related standards and recommendations of ITU-T, ISO/IEC, and IETF. The latest version of the X.509 ITU-T recommendation [15] specifies the format of an attribute certificate (currently in version 1). This certificate is a separate data structure from the public key certificate of the subject, but it is logically bound to the public key certificate.

According to the ITU-T recommendation, an attribute certificate may be is-

sued by a different entity than the entity (*Certification Authority*,CA) issuing the associated public key certificate. This new authority is the *Attribute Authority* (AA), which assigns privileges to users by issuing the corresponding attribute certificates. Thus, the attributes of a final user are digitally signed and its certificate issued by an AA, whose attributes are in turn signed and certificate issued by another AA. Chains of attribute certificates can be built recursively. In fact, the recommendation defines a framework that provides a foundation upon which a *privilege management infrastructure* (PMI) is built. The use of attribute certificates has an additional important advantage because it allows, under certain conditions, to fulfil privacy requirements too, as demonstrated in [17].

Most of authentication and authorization services focus on either authentication or authorization, and are not complete. It is necessary to extend the scope of security solutions by providing an integrated authentication-and-authorization service for communicating peers; that is, to create an *Authentication and Authorization Infrastructure* (AAI) [16].

Using an AAI, a user typically registers only once in his or her home domain. When the user requests a resource, he or she should always be authenticated by his or her home domain, and the request should be forwarded to the destination server complemented with some additional information (provided by the user's home domain authentication server). Consequently, the challenge of an AAI is to provide an inter-domain authentication and authorization service.

4 Description of our Methodology. A Case Study: PASEN

In this section we show our methodology to establish a use case-driven software development framework based on the UML. This methodology integrates security requirements into a business process model of the system. We also explain how to introduce the advanced security services; more precisely, the Authorization and Authentication Infrastructures explained in previous section, in order to fulfill properly the security requirements.

For a better understanding, we use as example the application PASEN, an e-government application developed in the framework of the European Project CASENET. This application is intended to enable the teachers, administrators and student tutors within an educational centre to manage their communication needs via a web portal. The services to be offered to teachers, administrative staff, parents and students, include basic services such as pre-admission, student's registration, and grant management. One of the main objectives of the final system will be to facilitate the tracking of the status of submitted requests, e.g. grant requests. The PASEN core activities that need

to be secured include student registration, grant management, pre-admission requests, homework, student absences, and examinations. Each user requires a profile to access to the PASEN portal. The main different profiles are tutors, teachers and several categories of administrators.

4.1 Exploring Security Requirements Phase

The UML is extended in order to express security notions. In order to represent business processes, we use the Eriksson-Penker extensions for business modelling with UML [12]. Use cases and the corresponding scenarios are used as the basic tool to build threat models and elicit security requirements. The latter are originally stated at a high level of abstraction within a functional representation of the system, thus yielding a security-enriched specification.

The expressiveness of the UML notation for specifying security properties has recently been the subject of hot debate among researchers. There is agreement that robust tools and techniques for enabling syntactic and semantic analysis of UML diagrams are essential. There is also widespread concern in relation to what appears to be shortcomings of UML, e.g. lack of formal semantics and of expressiveness for modelling security properties. However, UML is considered to be attractive to a broader community with less critical security requirements. Many researchers are currently developing methods to bridge the gap between UML and formal specification languages and analysis tools.

Together with an extensive tool support, UML has become a de facto industry standard, and the development of techniques for enabling UML users to apply formal analysis tools also talk in favour of UML. Moreover, the simplicity of UML modelling notations facilitates the capture of abstractions for a variety of domains, including security-critical systems. Most importantly, UML offers an opportunity for researchers to apply formal methods on a top-down basis, thus increasing the probability that these methods be adopted in an industrial setting.

We concentrate here on the grant management service. This activity consists of a part dealing with grant application and another with the grant follow-up. The tutor may apply for a grant by filling in and submitting a grant form. Once submitted, he receives a reference number that can be used to obtain the information from the grant follow-up, which is provided by the administrator of the educational centre. A sequence diagram for this service is shown in Figure 1. The steps in the sequence diagram are explained in Figure 2. As we may observe, this diagram does not specify any security requirements, only the functional ones. It corresponds to a high level use case or a core business process, and must be decomposed several times during the software

development process. This type of representation is one we may expect from system developers, and offers a good setting for studying and eliciting the required security properties of the system.

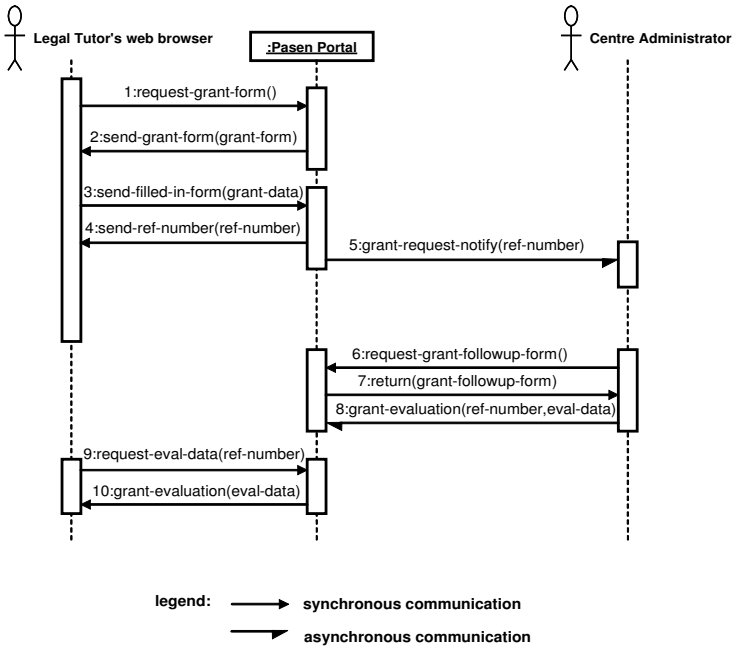

Fig. 1. Sequence diagram for grant management

1. The PASEN User (PU) using a web browser (WB) requests from the PASEN Portal (PP) a grant application form.

2. PP sends to WB a grant application form.

3. WB sends to PP the grant data, i.e., the filled out grant application form plus any other needed document.

4. PP sends to WB a reference number to be used as an identification of the submitted grant application.

5. PP sends the grant data to the Centre Administrator (CA) in charge.

6. CA requests a grant follow-up form from PP.

7. PP sends to CA the grant follow-up form.

8. CA sends to PP result from the evaluation of the grant, i.e. the evaluation data.

9. PU via the WB requests grant information from PP.

10. PP sends to PU the grant evaluation.

Fig. 2. Steps of the sequence diagram

The security requirements associated with this service turn out to be extensive. Some are of a more general character, while others are related to the information exchanged during interactions: the grant application form, the grant

data returned in the application (the filled application form), the reference number, and the evaluation data. In a general manner for the grant management, we need: (i) a security service allowing the notarisation for each type of non-repudiation proof, and (ii) a security service that provides a unique temporal reference. More particular requirements are as follows.

The integrity of the application form is required. Therefore, we need a security service that allows verifying if an unauthorized modification of information (including changes, insertions, deletions, and duplications) has not occurred either maliciously or accidentally.

Concerning the grant data, both integrity and privacy are required. As a result we need a security service here that apart from guaranteeing data integrity, as above, also provides privacy, avoiding any unauthorized access or any disclosure of information. As for privacy requirements, it should be possible to verify whether any form of unauthorized modification (including changes, insertions, deletions, and duplications) has occurred either maliciously or accidentally. Moreover, the different actors involved should be able to sign the grant file because this file is regarded as a specific contract. Once signed, it is required that the contract cannot be modified. Finally, a security service is required that provides a proof of the grant evaluation submission. The reference number should also be protected. Integrity and privacy are both required, as well as proof of reception of the reference number.

Although the application is rather standard and simple, the security requirements, taken together, are very complex. The requirements are hard to meet if they are added as an afterthought to the developed system. The complexity increases if moreover flexible solutions are required, e.g. if several similar systems exhibiting different sets of security requirements should be developed. In addition, the requirements may change during the lifetime of the deployed system. The need for a precise method to develop this kind of security-critical system becomes evident here.

As we may observe, the security requirements of the PASEN application refer to several perspectives. These perspectives can be associated with different types of UML diagrams. Hence, the functional perspective corresponds basically to activity, use case, and sequence diagrams. The static perspective corresponds mainly to class diagrams, the dynamic perspective to state charts, the organizational perspective to lanes in activity diagrams, class diagrams and packages, and the business process perspective to process models. All these diagrams can be affected by the security requirements. Our approach is to begin by encoding the functional aspects of the system in the different diagrams, and then to extend these diagrams in a variety of ways in order to express the corresponding security requirements. These extensions should be easily understandable by domain experts, and should as far as possible be

based on standard definitions of security concepts. As an example, a security enriched use case, using a scheme shown in [13], could turn out to be as shown in Figure 3.

Use case: Grant Management

Functional Summary: A tutor requests a grant and an administrator of the educational center returns a grant evaluation.

Actor: tutor, administrator.

Security subject: tutor: authenticity, authorization, privacy.

Preconditions: Tutor authenticated and authorized.

Security objects:
- grant form: integrity
- grant data: integrity and privacy
- reference number: integrity, privacy, non-repudiation of reception by tutor
- evaluation data: integrity, privacy, authentication of origin, non-repudiation of reception and submission

---

Fig. 3. Security enriched use case

The corresponding business process diagram integrates several perspectives and includes an input object, an input event executed by a tutor, and input data. The output is a grant evaluation. Omitting many details, the purely functional version of the Grant Management process, i.e. without the security requirements, could be schematically represented as shown in Figure 4. The two subprocesses in the grant management process correspond to the Grant Application resp. the Grant Follow-up subprocesses.

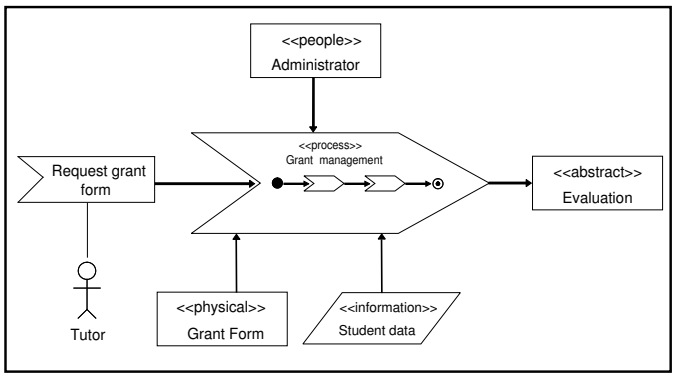

Fig. 4. Grant management business process

The Grant Management process extended with security could be described as shown in Figure 5, where irrelevant details are left out. In this diagram we introduce a new element, stereotyped by <<security>>, which can be interpreted as a kind of security goal. In the lower rectangle of each element we include the parameters associated with the security goal, stated in an informal way.

The next step would be to integrate the security goals into the business process itself, which might result in extensive changes to the previous flow of events and activities, including the addition of new subprocesses. Non-repudiation, for instance, may require the inclusion of new actors, e.g. trusted third parties, and new types of information objects and activities may also be required. The resulting business process should ideally be based on solutions contained in the repository, and be the result of a pattern-based analysis applied to the security-enhanced business process shown in Figure 5. A similar procedure, with similar results, can be applied to the corresponding sequence diagram, thus yielding a new sequence diagram that might include e.g. communication between the original parties and a trusted third party, e.g. an e-notary. Other diagrams corresponding to distinct perspectives may also require changes in the same spirit.

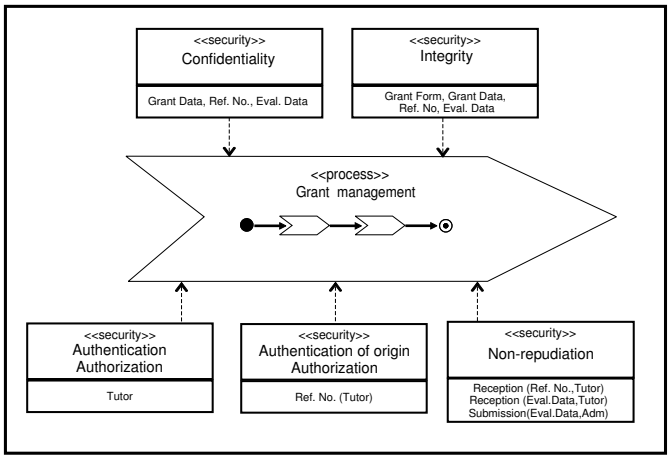

Fig. 5. Security enriched grant management

A process corresponds to a procedure defined at some level of abstraction, and this procedure may change during the lifetime of a system. A subprocess needs not represent a purely internal activity, it may very well communicate with agents outside the organization, and may even be allocated to a party outside the organization. The advantage of having a uniform representation of the several views of the system and its parts is that inconsistencies arising from these complex phenomena might become visible at any stage of the software development life cycle.

An important question here is how the security goals associated with business processes relate to process decomposition. In Figure 5 we have a process, Grant Management, which consists of two subprocesses in sequence. Several security goals are associated with the parent process. The goal of authenticity can be assumed to apply to the two subprocesses in the same way as to the parent process. By contrast, non-repudiation is a kind of security goal that does not decompose into two identical goals, one for each subprocess. It may require a complete solution at the parent process level. There is no general solution to

the process decomposition problem with regard to with security requirements. Only a case by case study of each security goal, supported possibly by a repository of previously worked solutions and a pattern-based analysis tool, seems to be feasible here

Once the business model is encoded into ConGolog, the main challenge is to express in this notation the security goals associated with the UML business process model, which in our example include non-repudiation, authentication, authorization, integrity, and privacy.

A domain expert can easily understand the security requirements expressed in the form exemplified in Figure 5, and might even have created them. It is however uncertain whether the developer would like to go further than this in the specification of the system requirements. The requirements might also have been partially generated from other views of the system, and consistency across different perspectives should be checked at this stage. The semantics of the expressions related to security should be as precise as possible, ideally based on some standard. The resulting solution should in any case be checked by the domain expert e.g. for validation, since it will probably have an impact on the overall functionality of the system and affect other requirements. Also, several forms of threat analysis can also be performed at this stage, for instance those based on use cases or scenarios. The final result is a specification of the system at a high level of abstraction including the security requirements, which becomes an input to the next stage of system development.

4.2 Introducing Advanced Security Services Phase

In the previous section we have explored the security requirements, obtaining the necessary security elements by using the Business Process Model designed.

A design of a system without the application of the techniques explained before would constitute a very poor solution. In fact, a design without the previous specification phase will probably take the designer to a wrong decision: the use of a traditional authentication system, like a password-based mechanism to authenticate users in the web, since that is a fast, cheap and technically simple solution. However, when making use of the previous specification, the designer will realize that the security requirements are more complex than expected, requiring not only the authentication service, but the non-repudiation service, based on the previous one. This will guide the designer to realize that a more complex security solution is needed; for instance, a PKI/PMI-based solution. Moreover, because of the privacy requirements, a solution of this type will be additionally useful for the designer when extending the use of attribute certificates as proposed in [17].

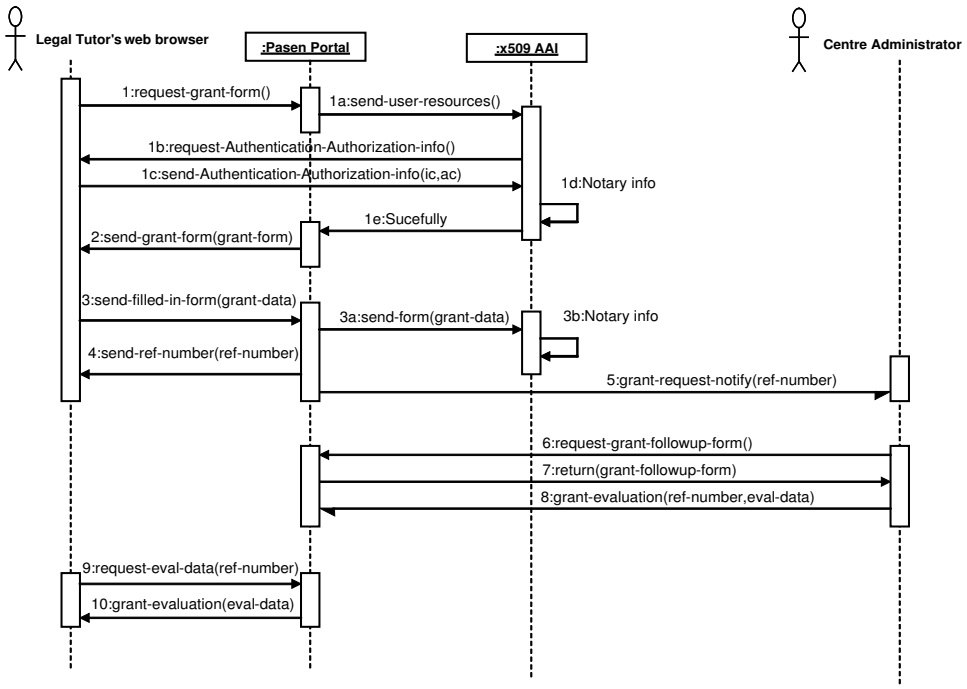

Fig. 6. Adding AAI Solution to sequence diagram for grant management

Another example can be seen when considering the authorization mechanism. A quick design will make the user to choose a common authorization system, that is, a system where a policy determines the allowed actions. However, this solution will present scalability problems when the number of users grow. Moreover, delegation procedures between management centers will not be achieved.

Therefore, by knowing beforehand, and in a precise way, the security requirements of the system as well as the level of security provided by every service, the designer will be able to select and apply the correct services. In other case, the incorrectly application of the services will produce an incorrect design and, consequently, an increment of the development costs.

The figure 6 is the result of introducing the AAI into the system described in the figure 1. The inclusion of this component allows to fulfill the security requirements inferred in the specification phase. The use of identity certificate enables the use of SSL protocol to authenticate both the Tutor and the PASEN portal. The user is identified as Tutor presenting the corresponding attribute certificate which details the rol of the user. Inside the management center the authorization policy collects the necessary attribute certificates to perform the authorization tasks. In addition, the AAI can be used as trusted third party, monitoring the flows of information from the communications. Integrity and privacy can be resolved using the pair of keys to sign and encode the shared information. Therefore, authentication, authorization, non-repudiation,

integrity and privacy can be solved, only including the AAI module as a black box.

5 Conclusions

In this exploratory study we have presented work intended to establish a use case-driven software development framework based on the UML, and to integrate security requirements into a business process model of the system. The UML is extended in order to express security notions. Use cases and the corresponding scenarios are used as the basic tool to build threat models and elicit security requirements. The latter are originally stated at a high level of abstraction within a functional representation of the system, thus yielding a security-enriched specification. In addition, an advanced authentication and authorization service is introduced. The service is based on the X509 ITU-T Recommendation. The resulting representation is translated into a formal notation like ConGolog for testing, validation and verification. This procedure is iterated as many times as required. The result is used as input to the following stages of system development. Finally, a brief description of the system including authentication and authorization services is presented, and we show how the interaction with other functional elements of the system.

6 Acknowledgements

This paper is an outcome of the work performed in three Research Projects where the different co-authors have been involved. We very much thank the support of: (i) the European Commission through the CASENET Project (IST-2001-32446), (ii) the Japanese National Institute of Information and Communication Technology (NICT) through the International Collaborative Research Project "Secure Privacy Infrastructure" and, (iii) the Spanish Ministry of Science and Technology through the project PRIVILEGE (TIC-2003-8184-C02-01).

References

[1] ISO/IEC, "Information technology Code of practice for information security management ISO/IEC 17799", 2000

[2] Gordon, Lawrence A.; Loeb, Martin P., "2004 CSI/FBI Computer Crime and Security Survey", Computer Security Institute, 2004

[3] D. Geer, M. Donner, M. Davidson, L. McGhie, A. Shostack, "Patch Management, Can't live it,can't live withour it", Secure Business Quarterly, 2003

[4] G. Tassey, "The Economic Impacts of Inadequate Infrastructure for Software Testing", National Institute of Standards and Technology, 2002

[5] National Institute of Standards and Technology, "Comon Criteria for Information and Technology Security Evaluation", U.S Dept. of Commerce, National Bureau of Standards and Technology,August, 1999

[6] OMG Document,"MDA Guide V1.0.1",2001

[7] BPMI Document, "BPML 1.0 Specification",2003

[8] IBM Corporation, "Business Process Execution Language for Web Services Version 1.1"

[9] WfMC,"Workflow Process Definition Interface–XML Process Definition Language (XPDL)", WFMC-TC-1025,WfMC Standards,2001

[10] Giuseppe De Giacomo and Yves Lésperance and Hector and J. Levesque, "ConGolog, A Concurrent Programming Language based on Situation Calculus", Artificial Intelligence, 2000

[11] W.M.P. van der Aalst, "The Application of Petri Nets to Workflow Management", The Journal of Circuits, Systems and Computers, 1998

[12] Hans-Erik Eriksson and Magnus Penker, "Business Modelling with UML: Business Patterns at Work", John Wiley & Sons, 2000

[13] Mikko Siponen and Richard Baskerville, "A New Paradigm for Adding Security into IS Development Methods", Advances in Information Security Management & Small Systems Security, Kluwer Academic Publishers, 2001

[14] R. Housley,W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", *Request for Comments 2459*, Network Working Group, Internet Engineering Task Force, January 1999.

[15] ITU-T Recommendation X.509, "Information Technology. Open systems interconnection. The Directory: Public-key and attribute certificate frameworks", March 2000.

[16] J. Lopez, R. Oppliger, G. Pernul, "Authentication and Authorization Infrastructures: A Comparative Survey", Computers and Security (accepted for publication).

[17] V. Benjumea, J. Lopez, J. A. Montenegro, J. M. Troya, "A First Approach to Provide Anonymity in Attribute Certificates, 2004 International Workshop on Practice and Theory in Public Key Cryptography (PKC'04), Springer-Verlag, March 2004.