A Model Driven Security Engineering Approach to Support Collaborative Tools Deployment over Clouds

(W. F. Ouedraogo)[1] , F. Biennier[2], P. Ghodous[3]

Abstract The development of web 2.0 increases the call for agile and simple business process support. SOA (Service oriented Architecture) provides companies a new model to build their IT applications around their business processes and to combine them dynamically with the services of partner companies. Moreover cloud computing offers new business models and deployment opportunities to support adaptive and scalable execution environment. However, to provide services collaboration from several companies, the security policy associate to each company must be respected. So, the Business Process (BP) provides by these companies services inter-connections should be adapted to the security policy of each company and to the platform where it will be deployed. This leads to propose a new platform based on MDE (Model-Driven Engineering) approach to allow companies to build and deploy safely their BP in the Cloud environments.

Keywords

Business Process, Cloud computing, Security model, MDE

[1] W. F. Ouedraogo (✉)
Université de Lyon, CNRS INSA-Lyon. LIRIS. UMR5205. F-69621. France, 20 Avenue Albert Einstein 69621 Villeurbanne cedex, France
e-mail: wendpanga-francis.ouedraogo@liris.cnrs.fr

[2] F. Biennier (✉)
Université de Lyon, CNRS INSA-Lyon. LIRIS. UMR5205. F-69621. France, 20 Avenue Albert Einstein 69621 Villeurbanne cedex, France
e-mail: frederique.biennier@liris.cnrs.fr

[3] P. Ghodous (✉)
Université de Lyon, CNRS Université Claude Bernard Lyon 1. LIRIS. UMR5205. F-69621. France, 43 Bd du 11 novembre, 69622 Villeurbanne cedex, France
e-mail: ghodous@liris.cnrs.fr

1 Introduction

To fit the renewed globalized economic environment, enterprises, and mostly SMEs, have to develop new networked and collaborative strategies. This involves increasing the IT support agility and interoperability and allowing to each company to “inter-connect” their Information Systems (IS) in order to create a collaborative system. This collaborative IS includes both data and Business process which come from different companies each has its own security policies. This challenges the IS design paying attention to “functional and organizational” security requirements identification before deploying them. At the same time, the opportunities provided by the XaaS and cloud economical models allow companies to take advantage of new Business models and scalable environments, and increasing also IT productivity while reducing IS management costs. Therefore, the Cloud model appears for the companies as a solution to build and deploy these collaborative environments. This outsourcing strategy also challenges security policy adaptation according to the “hosting platform” vulnerabilities. To fit both challenges, it is necessary to provide a collaborative platform to allow companies to build collaborative environments and deploy them into the Cloud taking into account the BP security requirement and the Cloud vulnerabilities.

To this end, after the related work, we present our approach based on a Model-Driven Engineering (MDE) to identify BP security requirements, define an adapted Quality of Protection and generate adapted security policies, paying attention on the deployment platform. Then we apply our approach with a use case study.

2 Related Work

The openness and flexibility provided by the Web 2.0 involves re-thinking the information system organization. The benefits offered by the web 2.0 allow moving from a global enterprise engineering strategy leading to Business with the Cloud based process. This challenges information system to set new “service–based organizations” taking advantage of interoperability and flexibility provided by Service Oriented Architecture (SOA). At the same time, cloud computing provides new opportunities to support agile and flexible deployment allowing sharing resources and taking advantage to XaaS business models. This leads to “rethink” both Business Process models in security architecture according to Cloud and XaaS visions.

2.1 Business process security engineering

Business Process (BP) [1] is a defined set of business activities that represent the steps required to achieve a business objective. It includes the flow and use of information and resources.

To build business processes, formalizing the collaborative processes, there are various types of modeling tools and languages such as BPMN (Business Process Modeling Notation) [1]. It is mostly used to describe flows between the different activities as well as "launching" conditions of a particular part of the process. It also helps to integrate the executable services to the process. While defining collaboration BP, one must pay attention to security requirement. Related to the specification of security requirements in business processes, [2, 3] are agreed to the idea that it is necessary to capture and include the business security expert point of view in the software development process specifications. This leads [4] to propose a BPMN extension that allows incorporating security requirements into business process diagram paying attention to both organizational and technical security constraints. [5] also proposes a new security language for BPMN process models. Nevertheless these basic needs must be adjusted to fit the corporate global security policy and pay more attention on vulnerabilities and threats analysis. In order to enforce the security requirement in business and application level, the security of infrastructure should be also required.

2.2 Security policy integration

Different methods can be used to set a consistent security policy, based on vulnerability and threats models such as EBIOS [6], MEHARI [7], OCTAVE [8, 9] and SNA [10]. However, none of them provide an end to end support for a security policy project (See Table 1).They are not user oriented, and don't fit the "dynamicity" required by the changing collaborative context nor provide any security patterns adapted to Cloud-based deployment.

Table 1 Comparison of some security methods

	Requirements Analysis	Design	Implementation
EBIOS	Identification of Risk and Objectives	Protection patterns	
OCTAVE	Identification of Structured Information Access	Best practices Objectives Prioritization	Audit and Implementation Project Management
SNA	Identification of Process and Resource Workflow	"Survival process" Design	CERT attacks information and knowledge base
MEHARI	Shortened Risk Analysis	Best Practices	Implementation of Project Management

2.3 Cloud security challenge

As defined by the NIST [11] Cloud is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”.

Depending on who owns the cloud and how the infrastructure information system components are shared (“virtualization level” namely IaaS, PaaS, SaaS, BaaS), different security challenges can be identified. Among these challenges the confidentiality (Third-party should not be access to sensitive information), the privacy control and the integrity of the data should be guaranteed depending of the hosting area regulation laws (see Table 2).

Table 2 Cloud deployment model and the challenge in each kind of cloud

	Challenges for data storage and confidence on the data.
Private Cloud	Confidentiality and integrity of the data should be guaranteed as for classical IS implementation.
	The third party is responsible of the consequences of any damages.
Public cloud	Ensure isolation of data for each customer and ensure that confidentiality and integrity of the data are guaranteed.
	Ensure also that the application of territorial laws [12] (e.g.: US Patriot Act [13], won’t compromise data confidentiality
Community Cloud	As companies don’t have the same security requirements, the challenge here is to enforce the security policies of each company
Hybrid Cloud	Combination of the different challenges that can be found in the others clouds.

To fit these security challenges, Jericho Forum has developed a cloud security cube model that allows companies to choose the type of cloud that is adapted to their business needs. This work [14] has identified four criteria to characterize cloud security depending on:

- *The data physical location* (inside or outside organization’s boundaries).
- *The technology* (proprietary or open source) witch impacts the interoperability and portability of Cloud data and applications.
- *The operating area* (Inside or outside IT perimeter).
- *The cloud provider* (Insourced or outsourced).

To fit security challenges and to provide a dynamic adaptation of the security policy to the runtime context, a multi-dimensional model should be set to integrate the cloud type and the XaaS virtualization level while defining the security requirement.

3 A Security Policy Generation Framework

Different studies have addressed cloud according to a technological point of view nevertheless this fit a “fixed” infrastructure. Our aim consists in taking advantage of the cloud elasticity and provides tools to generate the convenient security protection.

Collaborative processes are seen as a composition of business services obtained from business service repository. In order to allow companies to build their own process, deploy it in cloud infrastructure and execute safely it without IT specialist intervention, we propose to use Model-driven engineering approach.

Our approach allows identifying security requirements, defining an adapted Quality of Protection and generating adapted security policies, paying attention on the deployment platform. In this approach, different meta-model are defined to describe the process and its security constraint based on the security requirements. A platform specific model is used to integrate constraints related to the Cloud deployment model. Weaving, these meta-models allow at the end to generate the security policies to annotate the service description (WSDL). Lastly, the convenient abstract security components are used as standard interface to invoke, at runtime, the required security (Fig. 1).

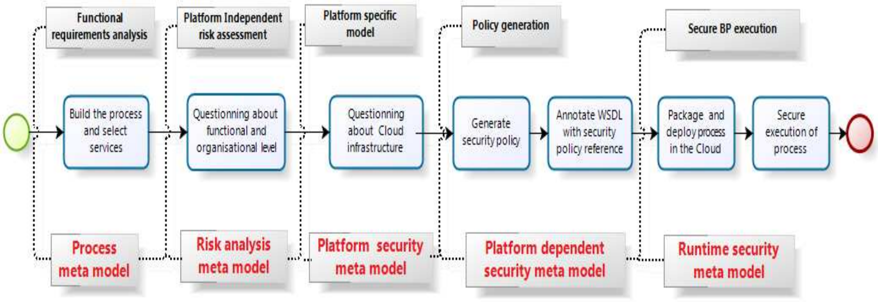

Functional requirements analysis
Platform Independent risk assessment
Platform specific model
Policy generation
Secure BP execution
Build the process and select services
Questionning about functional and organisational level
Questionning about Cloud infrastructure
Generate security policy
Annotate WSDL with security policy reference
Package and deploy process in the Cloud
Secure execution of process
Process meta model
Risk analysis meta model
Platform security meta model
Platform dependent security meta model
Runtime security meta model

Fig. 1 Approach to secure BP

3.1 Model driven security engineering method

As shown in Fig. 1, our security engineering strategy includes 3 steps:

- *Functional requirements analysis* allows designing the process workflow as a set of interconnected BPMN activities, supported by services WSDL.
- *Platform Independent risk assessment* is performed on the workflow specification. A set of questions/answers is used to analyze the different assets (process, services, and attached data) according to*:*

- *Functional security* deals with the kind of data handled by the asset and includes “legal constraints” regarding personal data and “patrimonial value estimation” as well the non-security costs estimation of the different assets. It also allows knowing intellectual property, strategic document for the company.
- *Organizational security* refers to the process organization (namely the actors and their role identification) and the invocation mode (on site / remote / mobile). It also allows knowing the confidentiality level (Top Secret, secret, Limited, Public...) and the Quality of Service (QoS) wished for each asset.

These steps are used to create a Platform Independent Security Policy: depending on the questions/answers, the BP security constraints are identified. This allows to select the corresponding security patterns and to insert security tags (related to basic security services taken from the OASIS security model [15] and protection level) in the WSDL specification.

- *Platform specific model* is used to integrate constraints related to the Cloud deployment model. Based on the security challenges that we identified in the Related Work Section, we build a Platform Dependent Cloud Security model. This vision incorporates both contextual management of non-functional properties (safety and quality of service) and management interfaces for specific data access. Risks and Security Patterns are identified in a 3 dimension model; paying attention on the basic security service introduced in the OASIS model, the Cloud model and the Virtualization (XaaS) level (Fig. 2). A set of questions / answers is used to identify the deployment configuration pattern according to this multi-dimensional model.

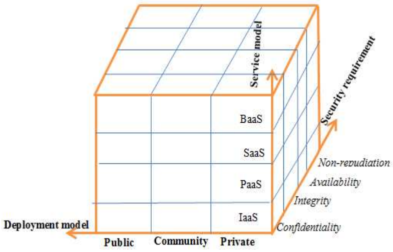


Fig. 2 Platform model.

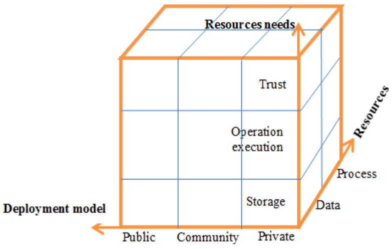


Fig. 3 Cloud model security requirements.

3.2 Policy generation

The *Contextual Security Policy* is used to describe the risk mitigation measures that must be implemented according to both the protection requirements and the particular vulnerabilities related to the platform model. Consequently, we first parse the security tags added in the service initial WSDL and combine them with the selected platform dependent pattern to identify the security components implementation patterns associated to either data or services regarding, trust management, operation execution of storage needs (Fig. 3)...Thanks to these implementation patterns identification, the platform independent tags are turned into real security tags according to the priority level associated to each requirement. Each tag refers to security policy files to apply.

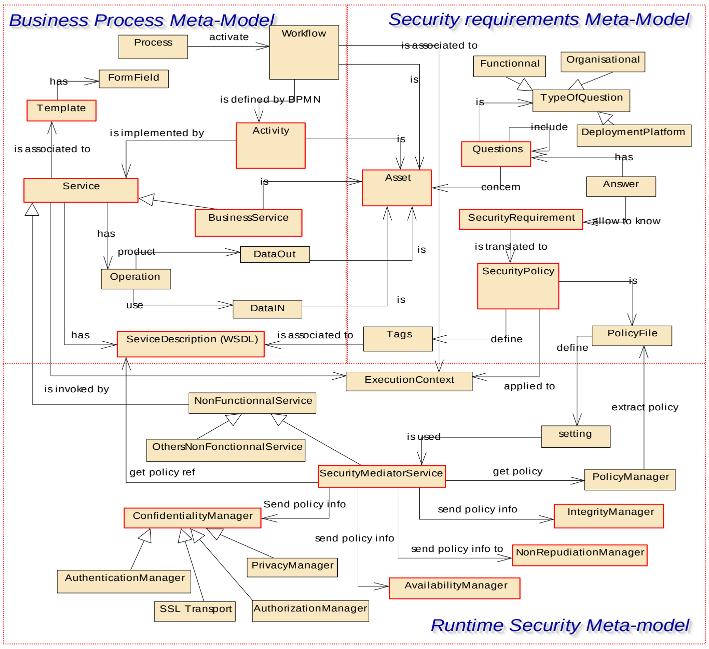


Fig. 4 Global security meta-model

3.3 Secure BP execution

At runtime, the security policy XML file is analyzed and used by the security mediator to invoke security components implemented as web service (security services):

- *Availability manager:* allows to access to a clone of the service if the requested service is unavailable or does not fit the QoS requirements.

- *The integrity manager:* ensures the data integrity during the message exchange.
- *The confidentiality manager:* includes an authentication service (used to identify the users), an authorization service that controls access to data and services, a privacy manager that manages the service/data storage by encrypting them.
- *The non-repudiation manager*: records the user's actions (authentication, access to the service, deleting of data…).

By this way, the secured services encapsulating the business services are deployed ensuring data security and the security exchanges.

The Global security meta-model illustrated in figure 4 shows the relationship between the process, the security requirements, the security policies and the security services.

4 Use Case

The purpose of our case study taken from [16] is to allow two companies to safely collaborate in order to produce an electrical connector. The connector includes electrical components, a protective insulation and a locking system. Company A is specialized in manufacturing of electrical system (electrical connector) and Company B in mechanical systems (protection (cladding product), locking system, insulation). Thus for every need of an electrical device in security system, Company A asks company B.

After asking company B to make the protection, a dialogue process between the two companies (project manager) occurs in order to identify the kind of protection system. Once the requirements analysis is achieved, each company designs the device helped by their designer and manufacturer team; protection device for B and electrical device for A. All devices are assembled by company B. The requirements analysis, the design and the production steps are represented as sub-processes. At the end of the process, data are archived by each project manager. The figure 5 illustrates the process.

To build this process we use our process meta-model which is a kind of BPMN model. The design platform is shared between the two companies and allows each company designer architect to define the process activities by searching in the services repository a service or sub process fitting the described activities (Fig. 5). At this step, the process is not secured.

To identify the security requirements, a set of questions (Table 3) related to the risk analysis model is submitted to the designers. These questions concern the process functionality and particularly the type of data manipulated by the process as well as the process organization (user's roles, user's connection).This allows securing the process at the functional and organization levels.

The last group of questions concerns the deployment environment to fit the infrastructure risk.

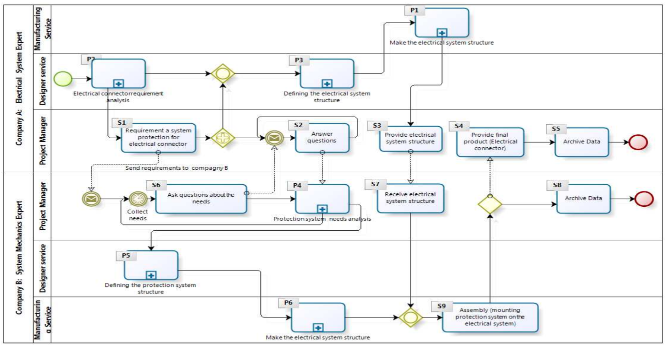

Company A: Electrical System Expert
Manufacturing Service
Designer service
Project Manager
Company B: System Mechanics Expert
Project Manager
Designer service
Manufacturin g Service
P1
Make the electrical system structure
P2
Electrical connectorrequirement analysis
P3
Defining the electrical system structure
S1
Requirement a system protection for electrical connector
Send requirements to compagny B
S2
Answer questions
S3
Provide electrical system structure
S4
Provide final product (Electrical connector)
S5
Archive Data
S6
Ask questions about the needs
Collect needs
P4
Protection system needs analysis
S7
Receive electrical system structure
S8
Archive Data
P5
Defining the protection system structure
P6
Make the electrical system structure
S9
Assembly (mounting protection system on the electrical system)

Fig. 5 Electrical connector production process

Table 3 except of questions

Security needs	Questions	answers
	Functional level protection	
C	Which services or process manipulate personal data?	Any services and process
C	Which services or process manipulate financial data?	Any services and process
C	Which services or process manipulate Strategic data (intellectual property, strategic documents...)?	Sub-Processes[P1,P3,P5,P6]; Services [S5, S8]
	What privacy level do you give to these strategic data? Top secret/ Secret/limited/Public.	Top secret
	Organizational level protection	
N	Are there services which exchange data which partners?	Services [S1, S2, S6]
C	Are-there services or processes which need to identify the user?	Yes. ALL
C	Do you need to filter the access of certain services or process?	Yes

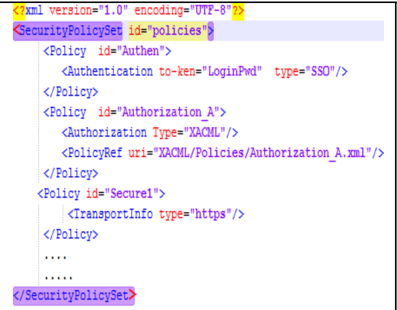
C	Must these services or process be invoked by a particular actor?	Grant (A.Designer, [S1,P2,P3]))
		Grant(B.Designer, [P5]))
		Grant(A.Maker, [P2]))
		Grant(B.Maker, [P6, S9]))
		Grant(A.Manager, [S1-S5, agreements (A.Designer, A.Maker)])
		Grant(B.Manager, [S6-S8,P4, agreements (B.Designer, B.Maker)]))

A	The availability level is important for you? If yes, which service and process do you need high availability	No
C, I, A	How the work station, which client capture data, is connected to the services? By internet / LAN /VPN?	Internet

Legend: C (Confidentiality), I (integrity), A (Availability), N (Non repudiation)

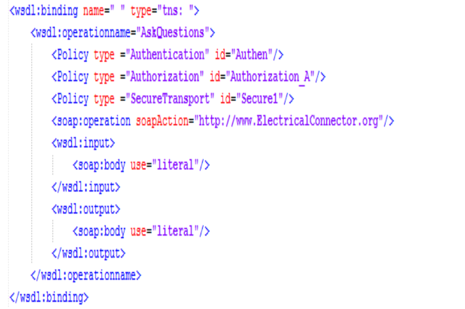
Each question is associated to assets (process, service, and data) and to the type of damage (loss of confidentiality, loss of integrity…). In our use case, we notice that the data archive services (S5, S8), designing processes and production manipulate strategic data considered as Top secret information so a high confidentiality level is required.

The S1, S2 and S6 services exchange information between companies, so these services need to store each user actions to avoid non-repudiation. Moreover all processes require authentication service and the access to each service should be controlled. The Managers have access to their own services and also to the designer and manufacturer services. The high availability of services is not a priority and users are connected thanks to internet.



```
<?xml version="1.0" encoding="UTF-8"?>
<SecurityPolicySet id="policies">
    <Policy  id="Authen">
       <Authentication to-ken="LoginPwd"  type="SSO"/>
    </Policy>
    <Policy  id="Authorization_A">
       <Authorization Type="XACML"/>
       <PolicyRef uri="XACML/Policies/Authorization_A.xml"/>
    </Policy>
   <Policy id="Secure1">
        <TransportInfo type="https"/>
    </Policy>
    ....
    .....
</SecurityPolicySet>
```

Fig. 6 Except of the process policies



```
<wsdl:binding name=" " type="tns: ">
   <wsdl:operationname="AskQuestions">
      <Policy type ="Authentication" id="Authen"/>
      <Policy type ="Authorization" id="Authorization_A"/>
      <Policy type ="SecureTransport" id="Secure1"/>
      <soap:operation soapAction="http://www.ElectricalConnector.org"/>
      <wsdl:input>
         <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
         <soap:body use="literal"/>
      </wsdl:output>
   </wsdl:operationname>
</wsdl:binding>
```

Fig 7 Except of “AskQuestions” service (S6)

These answers are used to generate a first security policy for these services as shown the Figure 1.6. SSO (Single Sign On) authentication and XACML (Access Control Markup Language) authorization are implemented to control data access, protected connection (https) are also used. The Figure 7 shows the annotation of the service “AskQuestions” WSDL.

Once the service is secured depending on functional and organizational requirements, the final questions set (Table 4) concern the deployment infrastructure characteristics.

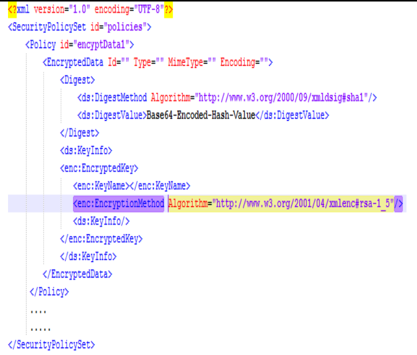
In our use case as the answers reveal perceptibly that the process which manipulates strategic data, will be deployed in public cloud. The data encryption is needed as data are stored outside the company IT perimeter and as the provider infrastructure is shared with other companies. (Fig. 8) shows the encryption policy added to the list of policy. This new policy is referenced in the WSDL on the archive manager service (Fig. 9).

Table 4: except of questions

Security needs	**Questions**	**answers**
	Deployment platform	
C	Who manages the Cloud infrastructure? You (the company) or the service provider?	The service provider
C	Where are data stored? Inside your company boundaries or outside	

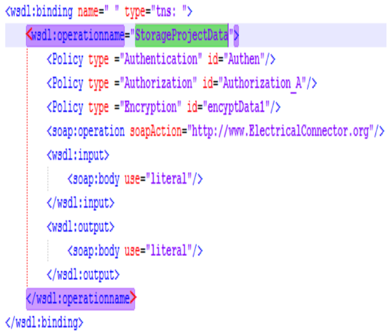
	outside.	
	Who owns the data? You (The company) or service provider?	The company
C	Is Cloud infrastructure shared to another's companies?	Yes

Legend: C (Confidentiality)



```
<?xml version="1.0" encoding="UTF-8"?>
<SecurityPolicySet id="policies">
    <Policy id="encyptData1">
        <EncryptedData Id="" Type="" MimeType="" Encoding="">
            <Digest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>Base64-Encoded-Hash-Value</ds:DigestValue>
            </Digest>
            <ds:KeyInfo>
            <enc:EncryptedKey>
               <enc:KeyName></enc:KeyName>
               <enc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
               <ds:KeyInfo/>
            </enc:EncryptedKey>
            </ds:KeyInfo>
        </EncryptedData>
   </Policy>
   ....
   .....
</SecurityPolicySet>
```

Fig. 8: Except of the process policies



```
<wsdl:binding name=" " type="tns: ">
    <wsdl:operationname="StorageProjectData">
        <Policy type ="Authentication" id="Authen"/>
        <Policy type ="Authorization" id="Authorization_A"/>
        <Policy type ="Encryption" id="encyptData1"/>
        <soap:operation soapAction="http://www.ElectricalConnector.org"/>
        <wsdl:input>
            <soap:body use="literal"/>
        </wsdl:input>
        <wsdl:output>
            <soap:body use="literal"/>
        </wsdl:output>
    </wsdl:operationname>
</wsdl:binding>
```

Fig. 9 : Except "ArchiveManager" service WSDL

After this analysis step, the security policies are generated. Lastly, process services are enriched with security components such as authentication, authorization, encryption and log.

During the execution, each invoked service will have its description (WSDL) parsed and the reference to the policies extracted, so that adapted security components (Authentication, Authorization…) are applied.

In our example, the call of operation "*StorageProjectData*" of service "*ArchiveManager*" is intercepted by a security stub. This security component analyzes the WSDL of service and extracts the authentication, encryption policies references. This leads to check of the authentication. If the user is not already identified (has no Authentication token), the Authentication service is contacted to identify the user. Then, the "*StorageProjectData*" calls the encryption service to protect data before encapsulating them in the secure transport service (https).

5 Conclusion

To fit the openness, interoperability and agility levels requested for collaborative business, we propose to organize a collaborative process design environment based on service composition. This design platform pays attention to the BP security requirements before deploying the secure BP on the cloud.

In this paper we present our model driven approach to define security requirements and generate contextual security policies depending on the hosting cloud characteristics. Based on security patterns selected thank to questions/answers, our solution allows a fast security reconfiguration according to the hosting platform. Thank to this approach, the platform proposed allows several partners to work together with respect for each security policy that applies in his company.

Further works will focus on the propagation of the security policies and detection of conflicts between the policies in order to ease the security specification process.

6 References

1. OMG (Object Management Group), (2011). Business Process Model and Notation (BPMN) Version 2.0, http://www.omg.org/spec/BPMN/2.0
2. Backes M, Pfitzmann B, Waider M (2003) Security in Business Process Engineering. In: vander Aalst, W.M.P., ter Hofstede, A.H.M., Weske, M. (eds.) BPM 2003. LNCS, vol. 2678, pp. 168–183. Springer, Heidelberg
3. Herrmann P, Herrmann G (2006) Security requirement analysis of business processes. Electronic Commerce Research 6(3-4), 305–335
4. Rodriguez A., Fernandez-Medina E., Piattini M., (2007) A BPMN extension for the modelling of security requirements in business processes, the institute of electronics, Information and Communication Engineers (IEICE), Vol.E90-D, NO.4.
5. Mülle J, von Stackelberg S, Klemen A (2011) Security Language for BPMN Process Models, Karlsruhe institute of technology, Germany.
6. ANSI (Agence National de la sécurité des SI), (2004). Expression des besoins et identification des objectifs de sécurité. La démarche", Version 2.
7. Club de la sécurité de l'Information Français (CLUSIF), (2010). MEHARI 2010. Guide de la démarche d'analyse et de traitement des risques.
8. Dorofee A (2002) Managing information security risks across the enterprise, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213.
9. Alberts, C., Dorofee, A., Stevens J., Woody C., (2003). Introduction to the OCTAVE Approach, Carnegie Mellon University, Pittsburgh.
10. Moore AP, Ellison R J, (2001) Architectural Refinement for the Design of Survivable Systems, Technical Note (CMU/SEI-2001-TN-008). Software Engineering Institute, Carnegie Mellon University.
11. Mell P, Grance T, J (2011) The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145
12. Sinclair J, Hudzia B, Lindner M (2011) The first International Conference on Cloud Computing and Services Science, CLOSER 2011 "Architecture for compliance analysis of distributed service based systems". Belfast, Northern Ireland, U.K.
13. US Government, (2001).Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act, Title V, s 505.
14. Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, Jericho Forum, Version 1.0, (April 2009), http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf.
15. Organization for the Advancement of Structured Information Standards (OASIS), (2009). OASIS: Reference Architecture Foundation for Service Oriented Architecture, Version 1.0.
16. Lima Dutra M, Ghodous P, Kuhn O, Minh T (2010) A Generic and Synchronous Ontology-based Architecture for Collaborative Design. Concurrent Engineering, Research and Applications 18(1):65-74, Sage, ISSN 1063 293X.2010.