25

SECURITY CONTROLS IN COLLABORATIVE BUSINESS PROCESSES

Jochen Haller, Yücel Karabulut, Philip Robinson
SAP Research, CEC Karlsruhe
Vincenz-Priessnitz-Str. 1
76131 Karlsruhe, Germany
[jochen.haller | yuecel.karabulut | philip.robinson]@sap.com

Virtual Organisations (VOs) are collaborative environments, encompassing different autonomous partners responding to a business opportunity with a focus on automation and flexibility. These are the sort of scenarios researched specifically in the EU IST project TrustCoM. Collaborative business processes are identified as the integrating component bringing together other required VO components and subsystems such as a policy infrastructure or contract management while still meeting the requirements regarding flexibility. eBusiness in such a complex, evolving environment as the one encountered in VOs can only prosper with an integrated security model, supporting various classes of VOs or catering for VOs forming in different business segments, for instance aggregated service provisioning or collaborative engineering. Such an integrated security model has to take the integrating component, collaborative business processes into account as well. This contribution deals particularly with the security model on the VO's enterprise layer. A business process model, offering means to controllably expose organisation internal processes is extended to interface with other security and contract management related VO subsystems (such as the policy infrastructure). The extended business process model supports process context aware security controls for and towards those subsystems within executable collaborative process instances.

1. INTRODUCTION

In today's economy, in many business areas, collaboration between organisations is becoming an essential requirement to meet business objectives. Collaboration between organisations typically involves extended negotiations between humans in order to come to terms with, for instance, a set of legal documents, formalising the collaboration in contractual form. Depending on the type of business objective, the collaboration has to be reflected to a varying extent on the Information and Communication Technology (ICT) layer as well. Some collaborations only require the exchange of simple communication, such as orders and invoices between collaborating partners' financial systems, while others require greater interaction like connecting supply chains across the administrative boundaries of organisations. In many business areas, speed and flexibility to adapt to dynamic situations is an important requirement to gain an edge on competitors. Involving supporting technologies from the ICT environment will help to meet these requirements.

In the above described ecosystem, the EU funded FP6 research project TrustCoM[1] investigates such collaborative environments which are termed as Virtual Organisations (VOs). A VO is defined as a temporary or permanent coalition of geographically dispersed individuals, groups, organisational units or entire organisations that pool resources, capabilities and information to achieve common business objectives. Since such a collaboration involves a great deal of exposure, in terms of an organisation exposing parts of its administrative domain, for instance confidential data or organisation-internal business processes, security requirements are of major concern. To make things even more complicated, otherwise independent organisations may even participate in more than one VO at a time where the VOs are in direct competition with each other. The presented work focuses on organisations participating in a VO, where their collaboration is covered by a contractual VO agreement. The inclusion and integration of Trusted Third Parties and external parties is not discussed within this paper. Neverthless, TrustCoM distinguishes different aspects of security and their management by the general term "TSC – Trust, Security and Contract – management".

- Trust - The collaboration has to be conducted in a reliable and dependable environment with partners having the same properties throughout the collaboration, e.g. based on reputation values.
- Security - The collaboration environment has to meet the security requirements of all participating partners and offer controls to monitor, adapt and enforce such requirements throughout the collaboration.
- Contracts - Contracts formalise the collaboration between partners and contract terms have to be enforced and monitored throughout the collaboration.

TrustCoM aims at developing a framework for enabling trusted, secure business collaborations in on-demand created, self-managed, scalable and highly dynamic Virtual Organisations.

Current VOs are supported in their collaborative efforts by at least partly available mechanisms on the service layer [10][11][12][13]. Currently missing is a strategy to coordinate these mechanisms. For example, consider the activation of a compensation mechanism, when a confidentiality requirement during enactment of a business transaction is violated using the optimal, minimal set of web service technology standards. How would this be specified using today's standards?

In this work, business processes on the top enterprise layer are foreseen as an integrating component, allowing for the optimal combination and configuration of service based TSC management mechanisms. Allowing for the business process to control TSC management on the service layer, we extended the chosen process model of Schulz et al. [7] by a so-called TSC task and a TSC context on the process level. In this paper we present the initial results of the extended collaborative business process model.

The rest of the paper is organized as follows. Section 2 presents the basic process model and introduces the Collaborative Business Process (CBP) model, including the description of the modelling methodology as far as necessary for the comprehension of the TSC task model. Section 3 exhibits the TSC management support in the CBP model and introduces the TSC task. Finally, section 4 analyses

[1] http://www.eu-trustcom.com

the related work, followed by section 5 concluding and providing an outlook on future work.

2. COLLABORATIVE BUSINESS PROCESSES

We introduce the Collaborative Business Process Model and the related modelling methodology in three phases, tailored for VOs. The following sections aim at executable Business Processes (BPs) which are executed at runtime in a business process execution engine.

2.1 Process Model

Business Process Management subsystem in TrustCoM plays a central role among other subsystems, such as the policy and monitoring subsystems, such that the modelling technique for business processes was chosen carefully to be aligned with the models created of other subsystems. Business processes are essentially comprised of tasks or activities executed in a coordinated order. The outcome or result of a task is able to influence the subsequent order of tasks in the process enactment. This ordering of tasks is represented as transitions between tasks. As depicted in Figure 1: Basic Process Model, business processes are modelled as UML activity diagrams [16].

The following components are the essential building blocks of processes:

Task: A task is the atomic business process component, describing an activity or altering the process' control flow, for instance splitting or joining the process flow. A process may contain different layers of detail. In the process model, a task can be an anchor or placeholder for a (sub-) process on a higher level of detail.

Transition or Arc: A transition is the second atomic business process component, connecting tasks with each other. Therefore, a transition always has a source and a destination. A transition is always unidirectional.

Figure 1: Basic Process Model illustrates the composition of the basic components in a simple business process. The diagram also contains a dedicated "begin" and "end" task. The process model can be visualised as a directed graph which is similar to the Business Process Modelling Notation (BPMN) [13] or various other established graphical BP modelling notations.

Figure 1: Basic Process Model

2.2 Collaborative Business Process Model

This basic model is extended to a process model catering for business process collaborations across administrative domains in a VO. The extension is based on work conducted in [7] on business process views in CBPs.

The following three classes of business processes are distinguished and modelled in three different phases of the derived modelling methodology:

Collaboration Definition Phase: The *Collaborative Business Process (CBP)* is the process describing the (message) choreography among different VO partners on the

highest level of detail in the VO. The CBP describes the way to meet the business objective.

Distribution Phase: *External Business Processes (or View Processes)* are derived from the collaborative business process. They map to tasks in a CBP assigned to one particular partner in the collaboration.

Deployment Phase: Since highly optimised and tailored *internal (private) business processes* are assets of VO participants, these processes have to be protected. In the deployment phase views and internal processes are mapped to each other, including modelling rules to ensure consistency between both. Collaboration in a VO means that such assets like internal business processes have to be exposed in some way, but not necessarily in an uncontrolled fashion when they are required to contribute to the VO business objective. Views are in this respect the exposure technique for internal processes and are deployed in the administrative domains of assigned partners.

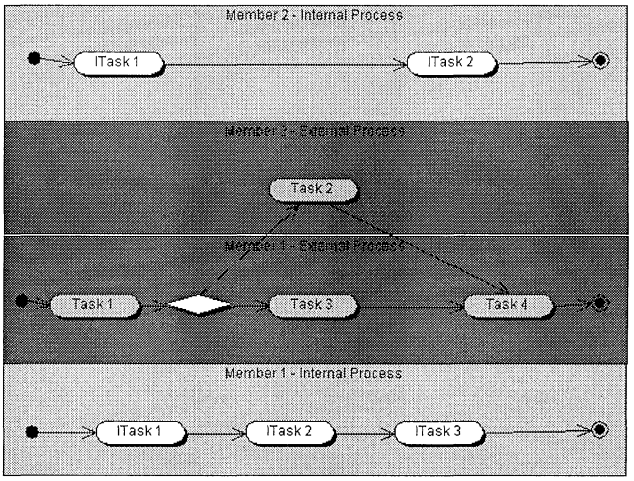

Figure 2: Basic concept of Deployment Modelling

Figure 2: Basic concept of Deployment Modelling shows a simple example of two collaborating partners with private business processes (outer swim-lanes) and associated views (external processes in inner swim-lanes). The CBP is not shown since such a choreography description is not required for enactment. In this example Member 1 chooses to expose all three internal tasks (iTask[1-3] in lowest swim-lane and corresponding Task[1-3] in swim-lane above) to the VO. The corresponding process view shows a mapping of all three tasks. Member 2 on the other hand wants to hide its two internal tasks (iTask[1,2] in top swim-lane). It only exposes the view task "Task 2", representing its two internal tasks, to outside administrative domains.

The described process model addresses security requirements in VO business process collaborations on a very basic level. Only exposure/privacy of entire private processes is addressed, which is not enough for realizing secure dynamic VOs. Secure business process enactment in a VO requires a more flexible security model that can dynamically react to events from other VO subsystems altering the process flow during runtime. Such events may originate from the monitoring subsystem,

generating notification events, or policy subsystem allowing adapted policies. The TSC task in the following section introduces a conceptual model created at design time of the business process to meet TSC requirements even during business process runtime.

3. TSC REQUIREMENTS IN COLLABORATIVE BUSINESS PROCESSES

The following TSC requirements are identified in TrustCoM and the mechanisms addressing those requirements are provisioned by different VO subsystems. The implementations of those mechanisms and functionalities are hidden behind a web service interface and can be invoked by task activities from within the business process level. The actual invocation is conducted by a so-called TSC task, an introduced BP modelling extension described in the following section.

Contract Management
Contracts in the form of Service Level Agreements (SLAs) play a central role in the set up and administration of a VO. Most parameters for VO management processes are derived from SLAs even during business process runtime in an automatic fashion.

Policy Management
Besides the basic message security requirements, authentication, authorization, integrity, confidentiality and non-repudiation, policies are an integral part to declare and specify more complex security requirements. Policies facilitate the understanding and enforcement of declared TSC requirements across and within administrative domains.

Trust Management
The concept of trust in TrustCoM mainly deals with reputation. During runtime, trust levels of e.g. VO participants have to be verifiable. Therefore, the notion of trust is based on reliable behaviour of partners participating in the VO. In case of erratic or unexpected partner behaviour, differences are measured against the expected behaviour fixed in an agreed upon contract.

3.1 The TSC Task

The TSC Task is an initially generic, neutral task that is modelled at design time in the collaborative business process whenever a TSC specific functionality during later process runtime is required. The specific task functionality, called a TSC extension role, can be assigned in either one of above described BP modelling phases (see section 2.2), or even deduced at runtime.
A TSC Extension Role is a TSC specific functionality to be assumed by a TSC task in the scope of a collaborative business process. Specific TSC functionalities lie in the area of above identified TSC requirements. TSC Extension Roles can be classified into trust, security and contract management or monitoring related functionalities, shown by their service interfaces on the service layer in Figure 3: TSC Task. The latter is emphasised because the previous subsystems report notifications through a monitoring subsystem and affect TSC Extension Role assignments during process instance runtime.

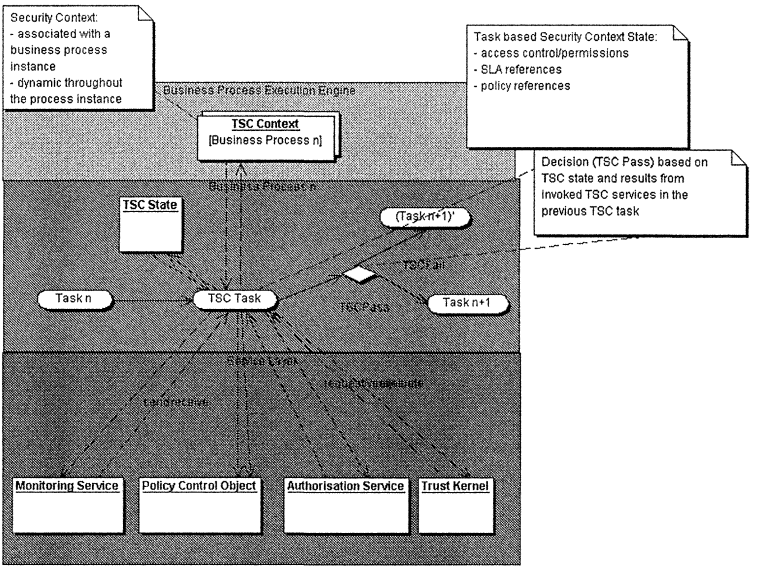

Figure 3: TSC Task

3.2 TSC Context

The TSC context captures the overall state of a business process instance and is used by the TSC task to fulfil its TSC extension role. The TSC context includes BP security control related metadata such as references to active policies or SLA's and provides interfaces to TSC Services like policy control object or SLA parser.

TSC extension roles are reflected in the TSC context content associated to a process instance. The TSC context content is the decision basis for TSC related control decisions during BP enactment, such as authorization, monitoring or policy adaptation decisions.

The TSC state captures, depending on the process configuration, the control decision relevant TSC context subset for a particular TSC task instance. Fields in the TSC context are conceptually modelled as task attributes. TSC tasks are intended to be used only locally, within one administrative domain and the lifetime of a particular TSC context instance is bound to the lifetime of a process instance. The TSC context by itself is designed not to contain confidential or security critical data, it is merely referencing such data, for instance active policies or access control lists which in turn are properly handled by their respective subsystems.

Figure 4: Business Process Component Classes summarises the described components and shows the overall UML information model of the presented work.

The upper half of the diagram shows standard building blocks of business processes, such as activities. Also, these building blocks are only shown on a higher level of abstraction. In more concrete business process models several elements would be refined and described in more detail.

The lower part illustrates the dependencies of the three phased modelling methodology and the TSC task (called also chameleon task) with related concepts in more details.

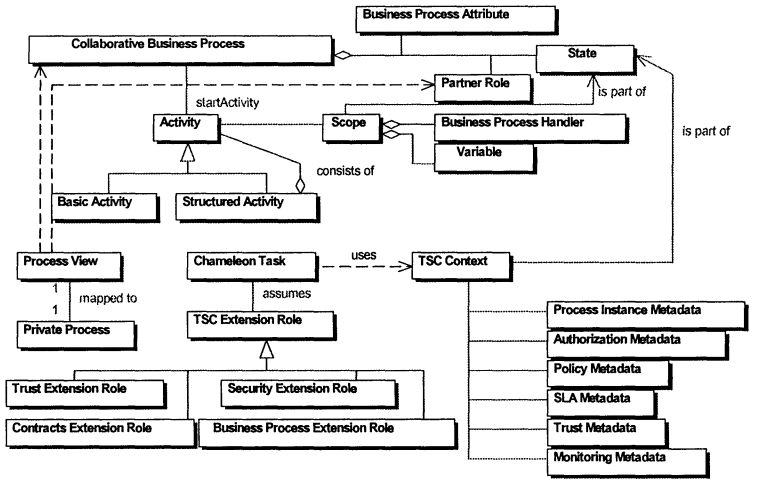

Figure 4: Business Process Component Classes

4. RELATED WORK

As mentioned above, the work introduced in this publication extends a collaborative business process model by Schulz et al. [7]. This work explicitly states security considerations as a high priority open issue. The authors of [8] and [9] independently worked on a view based process model and provide means to expose private processes, as a whole, in a controlled fashion to collaborating partners. This work still lacks an integrative component for process collaboration across administrative domains.

Executable processes in particular are addressed in [4] and [5], stating security requirements within business processes during enactment on the granularity of tasks, but focussing on authorisation. A generic model for more general security or even TSC requirements is not provided.

The work in [2] and [3] also remains with security as an authorization problem, but introduces already a SOA. The BPs are conceptually located on top of a (Web) Service Layer.

Different standards are available to model executable business processes. In [1] and [6] authors focus on BPs specified in the Business Process Execution Language (BPEL) [17] and addresses security requirements expressed as policies. BPEL specified processes, by language definition, require a SOA underneath and this work extends the scope of security requirements from authorisation decisions to policy requirements by means of service standards such as WS-(Security)Policy [12].

5. FUTURE WORK AND CONCLUSION

We introduced a conceptual model of the so-called TSC task addressing Trust, Security and Contract Management requirements in Collaborative Business Processes. The TSC Task leverages security related subsystems on a service layer by

providing security controls within business processes. The TSC Task is embedded in an also described BP model and methodology.

The described work is not yet complete and has to be considered as a snapshot of ongoing work. The BP modelling is conducted within the TrustCoM project as a continuous effort throughout the entire project lifetime of three years. This snapshot was taken after the first year of work.

The next steps will include a refinement of the deployment model, including conflict resolution when TSC tasks are inserted in the three methodology phases and when TSC Extension roles are assigned. An initial TSC Context specification is already available, but has to be refined and evaluated against the TSC subsystems. An interesting development is pursued by including (a subset of) the TSC Context in the synchronisation messages of enacted process views across domain using standards such as WS-Coordination [13]. An implementation of the CBP model and methodology is under construction, comprised of a modelling tool and BP engine, which will be tested in the TrustCoM framework implementation with other implemented TSC subsystems. The framework evaluation will closely follow emerging technology standards, such as WS-CDL, the Web Service Choreography Description Language [15], and comparably mature ones, such as BPEL [17].

REFERENCES

1. Stefan Tai, Rania Khalaf, and Thomas Mikalsen. "Composition of Coordinated Web Services". IBM, 2004.
2. Leune, Kees. "EFSOC Framework Overview and Infrastructure Services". Infolab Technical Report, 2003.
3. Leune, Kees. "A Methodology for Developing Role-Based Access/Control to Web-Services". Infolab Technical Report, 2002.
4. John A. Miller, Mei Fan, Amit P. Sheth and Krys J. Kochut. "Security in Web-Based Workflow Management Systems". Technical Report #UGA-CS-LSDIS-TR-99-010, 1999.
5. R. K. Thomas, R. S. Sandhu. " Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management". IFIP Workshop On Database Security, 1997.
6. Mendling Jan, Strembeck Mark, Stermsek Gerald, Neumann Gustaf. "An Approach to Extract RBAC Models from BPEL4WS Processes". WETICE, 2004.
7. Karsten Schulz, Maria E. Orlowska. „Towards A Cross-Organisational Workflow Model". Pro-VE, 2002.
8. Liu Duen-Ren, Shen Minxin. „Workflow Modeling for Virtual Processes: an Order-Preserving Process-View Approach". Information Systems 28(6), 2003.
9. Dickson K.W. Chiu, Shing-Chi Cheung, Kamalakar Karlapalem, Qing Li and Sven Till. " Workflow View Driven Cross-Organizational Interoperability in a Web-Service Environment". (ACM) Inf. Tech. and Management, 2004.
10. OASIS. URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss, 2005.
11. IBM/Microsoft/... URL: http://www-106.ibm.com/developerworks/library/specification/ws-trust/, 2005.
12. IBM/Microsoft/... URL: http://www-128.ibm.com/developerworks/library/specification/ws-polfram/, 2005.
13. IBM/Microsoft/... URL: http://www-128.ibm.com/developerworks/library/specification/ws-tx/#coor, 2005.
14. BPMI.org. URL: http://www.bpmn.org/, 2005.
15. W3C. URL: http://www.w3.org/TR/2004/WD-ws-cdl-10-20040427/, 2005.
16. OMG. URL: http://www.uml.org/, 2005.
17. OASIS. URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel, 2005.