Towards a Compliance-Aware Inter-organizational Service Integration Platform

Laura González and Raúl Ruggia

Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Uruguay
{lauragon,ruggia}@fing.edu.uy

Abstract. Organizations are increasingly required to collaborate with each other in order to achieve their business goals. The service oriented paradigm is currently the preferred approach to carry out this collaboration as facilitates interconnecting the software systems of different organizations. More concretely, such integration is supported by integration platforms which are specialized middleware-based infrastructures enabling the provision, discovery and invocation of interoperable software services. On another hand, these integrated and collaborative environments (e.g. e-government, e-health, e-science, e-commerce and e-business) must comply with regulations originating in laws, sectorial regulations, service level agreements and standards, among others. This research aims at proposing solutions to monitor and enforce compliance requirements in inter-organizational service integration platforms. Particularly, this work addresses compliance requirements on services, information exchanged and the flow of interactions between organizations. The solutions, which are based on well-known enterprise integration patterns and other capabilities (e.g. adaptability and context-awareness), are then refined into specific middleware technologies, notably Enterprise Service Bus and Complex Event Processing engines.

Keywords: regulatory compliance, enterprise service bus, complex event processing, service-oriented computing, enterprise integration, middleware.

1 Introduction

Over the last decades organizations have become distributed and dynamically federated entities which increasingly need to collaborate with each other by integrating and composing business services [1]. To achieve this, integrated software systems that implement such business services have become a must, as they enable to exchange data and execute business functions across organizations. This trend has led to large scale information systems which interconnect the software systems of different, autonomous and geographically distributed organizations sharing common goals [2][3][4]. This kind of systems can be found in different application domains such as e-government, e-health, e-science, e-commerce and e-business, among others [5].

In this context, the service oriented paradigm is currently the preferred approach to carry out multi-organization collaboration by allowing the integration and composition of distributed software services [4]. Such service integration is supported by the

R. Meersman et al. (Eds.): OTM 2014 Workshops, LNCS 8842, pp. 8–17, 2014.

so-called integration platforms, which are specialized infrastructures including an intermediate processing layer that facilitates the provision, discovery and invocation of interoperable software services. This intermediate processing allows performing validations (e.g. on access control policies), monitoring service invocations (e.g. on response time) and solving integration issues (e.g. communication protocol mismatches). Integration platforms are based on advanced middleware technologies, notably Enterprise Service Bus (ESB) and Complex Event Processing (CEP) engines.

Examples of large scale software systems supported by service integration platforms (SIP) can be found in e-government [6] and e-health [7] initiatives. In particular, the Uruguayan E-government Platform [6] includes an Interoperability Platform (InP) which facilitates the implementation and usage of e-government services based on a statewide service-oriented architecture (SOA). Indeed, by leveraging the Web Services technology, public agencies can offer their functionalities through interoperable software services, which are usually hosted on agencies' servers and exposed through proxy services in the InP. This way, all service invocations pass through the InP allowing to apply on them security controls and mediation operations (e.g. intelligent routing, message transformation). Fig. 1 presents a general overview of the InP.

Fig. 1. Uruguayan E-Government Interoperability Platform

Furthermore, the advent of cloud computing introduced the need for cloud-based integration alternatives involving a trusted intermediary party which provides solutions for different cloud integration requirements (e.g. cloud to on-premise, cloud to cloud, on-premise to on-premise [8]). These cloud-based SIPs, which support integration scenarios within and across organizations, can take different forms (e.g. Internet Service Bus [9], Cloud Service Broker [10] and Integration Platform as a Service [8]).

On another hand, these integrated and collaborative environments have to satisfy regulatory compliance requirements, originating from laws (e.g. personal data protection laws), standards and code of practice (e.g. HL7, WS-Interoperability), sectorial regulations (e.g. Sarbanes-Oxley, HIPAA) and service level agreements (SLA), among others, that apply to each organization as well as to the entire system [11]. Furthermore, in recent years, enforcing such compliance requirements (i.e. taking actions to assure their fulfillment) has become increasingly important, particularly in scenarios involving inter-organizational interactions. This is due to the fact that the non-adherence to these requirements may lead to the malfunction of the whole system and even may face organizations to litigation risks and even criminal penalties [12].

In particular, in the previous e-government scenario there are many compliance requirements that public agencies have to fulfill. For example, in order to improve the interoperability level, the Web Services provided by the agencies have to adhere to various WS-I profiles (http://www.ws-i.org/). Also, the information interchanged between public agencies cannot infringe the Uruguayan personal data protection law (http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331). Lastly, services have to be compliant with the SLAs (e.g. regarding response time, availability and throughput) that are established when they are registered in the platform.

Despite the relevance of these issues, current solutions addressing them are limited in terms of flexibility, agility and maintainability [12] and they do not address inter-organizational contexts [13][14]. In turn, given the mediation role of SIPs in inter-organizational interactions, these platforms are very suitable to perform the monitoring and enforcement of certain types of compliance requirements. Therefore, this work aims at proposing solutions to monitor and enforce compliance requirements based on SIPs and focusing on inter-organizational contexts. In particular, it addresses compliance requirements of services, information exchanged by organizations and the control flow of interactions between organizations. These solutions, which are based on well-known enterprise integration patterns (EIPs) and other specialized capabilities (e.g. adaptability and context-awareness), are then refined into specific middleware technologies (notably ESB and CEP Engines), types of regulations (e.g. data protection regulations) and application domains (e.g. e-health and e-government).

Then, the research questions for this work are: RQ1) Which are the most common families of compliance requirements in inter-organizational contexts?, RQ2) How can these compliance requirements be specified?, RQ3) Which capabilities should SIPs include to monitor and enforce these families of requirements? RQ4) How would a reference architecture for this platform be?, RQ5) How can the required capabilities be built by leveraging native features of middleware technologies like ESB and CEP?, RQ6) What are the potential and limitations of these technologies to carry out the required tasks, and how can they be extended or complemented?, and RQ7) Are current middleware products mature enough to implement the required tasks?

The expected contributions of this work are, firstly, academic, by proposing, specifying and evaluating novel integration technologies with specialized features to monitor and enforce compliance requirements in inter-organizational contexts. This is an open area [13] which is becoming more relevant with the advent of cloud-based integration solutions [8]. Also, the results of this work would be applied in real-world large-scale collaborative software systems (e.g. e-government, e-health) to allow a more efficient development and delivery of reliable public services.

The rest of the paper is organized as follows. Section 2 presents related work and Section 3 presents the research hypotheses. Section 4 presents the leveraged material and Section 5 describes the methods and work plan. Section 6 presents preliminary results and section 7 describes the evaluation methodology and contrasts the proposed solutions with existing work. Finally, Section 8 presents conclusions and future work.

2 Related Work

Various initiatives and projects have addressed regulatory compliance issues in service-based systems within organizations and, more recently, across them.

One of the most relevant projects in this area is the European project COMPAS [15] that proposes an integrated solution for runtime compliance governance in SOA which includes tools for modeling compliance requirements, linking them to business processes (BPs), monitoring process execution using CEP techniques, displaying the current state of compliance and analyzing cases of non-compliance [16][17]. However, the project mainly focuses on orchestrations (i.e. BPs managed within a single organization), while our solutions also address compliance requirements within a flow of interactions between organizations (e.g. choreographies). Also, although performing corrective actions is mentioned [17], the project mainly deals with monitoring tasks while our work also addresses enforcement tasks.

As the previous project, other proposals also focus on orchestrations and on monitoring tasks. In [18] an extension to a methodology called "architecture for BP optimization (aPro)" is proposed. This extension addresses the automatic generation of CEP rules to deal with the challenges of the runtime checking of compliance requirements in BPs. Also, in [19] a method for monitoring control-flow deviations during process execution is proposed. Its main contribution is a formal technique to derive monitoring queries from a process model, so that they can be directly used with CEP.

There are also proposals to deal with compliance requirements of choreographies. In [20] a Multi-source Monitoring Framework is proposed, through which the non-functional properties of choreographies can be monitored. Compared to our approach, this work only has detective purposes. Also, in [21] an architectural framework to verify the compliance of the overall sequence of inter-organizational choreography operations is proposed. Leveraging CEP, the solution uses event patterns to filter, monitor, and check for the incoming and outgoing calls. The solution performs preventive actions by filtering messages that do not comply with the requirements. Our proposal also deals with this kind of requirements, but it is not restricted to only that.

Other proposals focus on specific regulations. In [22], a proposal to enforce compliance with data privacy regulations in a health-related cross-organizational context is proposed. The authors propose an event-driven architecture based on an ESB and domain-specific languages (DSLs) to manage the elicitation and enforcement of data privacy rules. The paper characterizes the roles of Data Producer, Data Consumer and Policy Enforcer defining the events and message exchanges among them. However, compared to ours, this work does not address mechanisms to dynamically enforce non-complying interactions and it does not cover either other types of regulations.

More recently, compliance issues in cross-organizational BPs are being addressed. In [13][14] a property of "compliability" is defined to characterize interaction models consistent with a set of compliance rules. This work focuses on design time checking of compliance rules related to control flow, while ours deals with run-time checking and also covers other requirements (e.g. data-related).

Regarding middleware-based solutions, most of the previous proposals leverage these technologies. However, our work considers their mechanisms as first class citizens and not merely as tools. This allows: i) explicitly leveraging them, ii) identifying their limitations and complementing or enhancing them, and iii) refining the proposed solutions into different middleware technologies (e.g. ESB) and products (e.g. Esper).

3 Research Hypotheses

To address the research questions, we start from the following research hypotheses:

- **Hypothesis 1 (H1).** There are suitable mechanisms (e.g. DSLs) to specify the most common families of compliance requirements within inter-organizational contexts, in particular, regarding services, information exchanged by organizations and the control flow of interactions between organizations. (RQ1)(RQ2)
- **Hypothesis 2 (H2).** A SIP supporting the following characteristics is able to monitor and enforce these families of requirements: enterprise integration and connectivity patterns [23][24], adaptability [25], advanced monitoring and context-awareness [26]. (RQ3)
- **Hypothesis 3 (H4).** A reference architecture for a Compliance-aware Inter-organizational SIP can be specified to cover large-scale (e.g. e-health) as well as cloud-based (e.g. e-science) inter-organizational scenarios. (RQ4)
- **Hypothesis 4 (H4).** The capabilities in H2 can be built with native or extended mechanisms provided by middleware technologies (e.g. ESB, CEP). (RQ5)(RQ6)
- **Hypothesis 5 (H5).** Current middleware products (e.g. JBossESB) provide a suitable foundation to implement the required monitoring and enforcement tasks for the identified families of compliance requirements. (RQ7)

There are solid grounds for these hypotheses based on the related work described above. However, the research questions address extended issues on each of the items that have to be further analyzed.

4 Material

The material to evaluate the hypotheses presented in Section 4 comprises: i) existing knowledge on SIPs and middleware technologies: it mainly consists in our previous work which focused on proposing adaptive SIPs [25], context-aware SIPs [26] and domain-specific SIPs [27][28]; ii) existing knowledge on regulatory compliance: it mainly comes from the related work described in Section 2, in particular, we highlight the results obtained in the COMPAS project; iii) real application scenarios focusing on specific e-government [6] and e-health [7] integration platforms along with standards (e.g. SOAP, HL7), codes of practices (e.g. WS-I, IHE), laws (e.g. personal data protection laws) and agreements (e.g. SLAs); iv) Event-B [29] as a formal method to specify the proposed SIP as well as the compliance solutions. Event-B provides suitable characteristics (e.g. events and refinements support) to specify this kind of systems, there are various experiences of its usage in similar contexts [30] and we have already used in previous work [28]; and v) prototypes, leveraging existing middleware products, and prototypes from our previous work [31]. These prototypes will allow performing a functional and non-functional evaluation of the proposed mechanisms, evaluating the potential and limitations of current middleware technologies, and identifying / proposing enhancements or complementary components for them.

5 Methods / Work Plan

A successive refinement approach is being followed starting with the identification of relevant families of compliance requirements in inter-organizational contexts, continuing with the characterization of a compliance-aware inter-organizational SIP and its capabilities, and finishing with an incremental analysis and specification of solutions for monitoring and enforcing those families of requirements and specific regulations.

Event-B [29] will be used to specify the integration platform and the proposed solutions. This method is highly suitable to formally specify event-based systems in successive abstraction levels, which directly supports the proposed refinement-oriented methodology. Also, the practical application of the solutions will be discussed in the context of e-government and e-health domains, focusing on personal data protection laws and on standards and codes of practice suitable for these areas.

Based on this methodology, the work-plan consists of: i) identify common families of compliance requirements within inter-organizational contexts (e.g. interaction flow), ii) identify / propose suitable mechanisms to specify these families of requirements (e.g. domain-specific languages), iii) identify the required capabilities to monitor and enforce these requirements within SIPs, iv) define a reference architecture for a compliance-aware SIP which cover large-scale as well as cloud-based inter-organizational scenarios, v) specify the compliance-aware SIP and its capabilities through suitable mechanisms (e.g. Event-B), vi) propose and specify solutions to monitor and enforce the identified families of requirements based on these capabilities, vii) refine the reference architecture and the solutions to different type of regulations (e.g. data protection laws), viii) refine SIP capabilities into native or extended mechanisms provided by middleware technologies, notably ESB and CEP, and ix) prototype and evaluate the proposed solutions, using concrete middleware products and covering specific application domains (e.g. e-government, e-health).

6 Preliminary Results

This section describes the general architecture of the compliance-aware inter-organizational SIP and its envisioned refinement through different abstraction levels.

Fig. 2 presents the high-level architecture of the proposed platform which may be hosted within a trusted party (e.g. a supervisory agency).

As in any integration platform, the interactions (e.g. service requests / responses) between the interacting parties (i.e. organizations) pass through the platform in the form of messages (e.g. SOAP messages). In addition, the platform processes the messages to verify their compliance with the configured compliance requirements and, eventually, performs suitable actions to enforce them. To this end, it is equipped with traditional (e.g. EIP) and specialized (e.g. adaptability) capabilities. It also includes specific solutions, built over the former, to monitor (e.g. the exchanged information) and enforce (e.g. by blocking an interaction) common families of compliance requirements. Leveraging these specific solutions, higher-level solutions for specific types of regulations (e.g. personal data protection laws) can be built and refined into different domains (e.g. e-health).

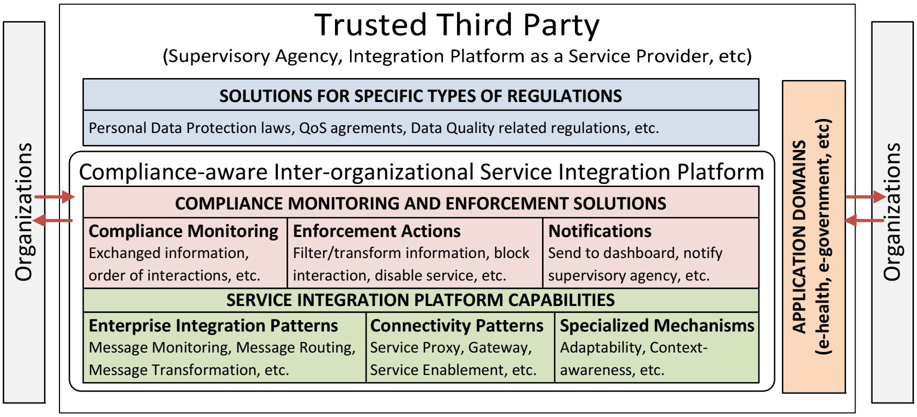

Fig. 2. High Level Architecture of the Compliance-aware SIP

Fig. 3 shows the different abstraction levels in which the compliance requirements, as well as the actions to be taken when a violation to them is detected, can be seen.

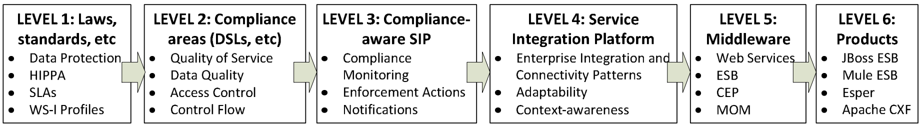

Fig. 3. Different Abstraction Levels

At LEVEL 1 there are the laws and standards which are usually specified in natural language. Some parts of them may be specified, by domain experts, using the mechanisms (e.g. DSLs) provided at LEVEL 2. If suitable mappings are set (between LEVEL 2 and LEVEL 3) the specifications at the second level may be automatically transformed into monitoring and enforcement solutions built on top of the solutions at LEVEL 3. As stated before, the latter are based on the capabilities of traditional SIPs (LEVEL 4) which can be, in turn, supported by different middleware technologies, such as ESB and CEP (LEVEL 5). Finally, the concrete implementation of these middleware technologies is provided by different products, such as Esper (LEVEL 6).

Note that the first four abstraction levels, and the mappings between them, support the agile development of compliance solutions by leveraging the proposed capabilities of the compliance-aware SIP (LEVEL 3). In turn, the last three abstraction levels provide the flexibility to implement a concrete compliance solution using different middleware technologies and products according to the specific context of use (e.g. scale of the solution, available resources). As a final remark, this work mainly concentrates on providing solutions and specifications for the third and fourth abstraction levels, along with the corresponding mappings with the second and fifth level.

Next, three examples are presented in order to illustrate the envisioned operation of the platform, focusing on the third and fourth abstraction levels.

Example 1: Personal data protection laws usually state that organizations cannot share sensitive personal data unless the person gives an explicit consent for that. In this case, the solution to monitor exchanged information (LEVEL 3) can be used to check if some sensitive data is interchanged without the corresponding consent. If so, and enforcement action can be taken (LEVEL 3), for example, to filter (i.e. take out) the sensitive data from the interchanged information before leaving the platform. This last action can be implemented at LEVEL 4 by the message transformation EIP.

Example 2: Two organizations agreed an allowed set of interactions and the order in which they have to take place (e.g. using BPMN2 at LEVEL 2) with the aim of carry out a collaborative business process. In this case, the solution to monitor the order of interactions (LEVEL 3) can be used. At LEVEL 4, this monitoring solution may be implemented using the temporal characteristics of CEP. If the order of interactions is not the agreed, the enforcement action to block an interaction can be taken (LEVEL 3), which is supported by the validate pattern (at LEVEL 4). The re-sequencer pattern (LEVEL 4) can also be used to return messages in the correct order.

Example 3: Some e-health regulations require that individual's health information has certain levels of data quality, in particular, regarding completeness. In this case, the solution to monitor the exchanged information (LEVEL 3) can also be used to check if the health information has the required level of completeness. If not, the enforcement action to transform the information (LEVEL 3) can be taken in order to complete the missing data. This is supported at LEVEL 4 by the enricher EIP.

Note that the platform will provide configuration options to manage the monitoring and enforcement of the regulations covered by the platform as well as to establish the application scope (one or several services, one or several organizations, etc.). These configurations have to be performed by business experts who know which could be the enforcement actions for a given regulation (e.g. block the interaction, modify the exchanged information) and the business implications of performing them or allowing non-complying interactions. Finally, there may be end-to-end requirements between organizations (e.g. confidentiality) that prevent monitoring and enforcing some compliance requirement at the SIP. Such cases would be analyzed as part of our evaluation activities with the aim of identifying the limitations of our proposal.

7 Evaluation and Discussion

The evaluation and validation of the results will mainly focus on: i) the capacity of the mechanisms to monitor and enforce the compliance of the identified families of requirements, which will be evaluated through the formal specification by showing that the solution correctly treats these requirements, ii) the development productivity and run-time efficiency of the proposed approach, which will be evaluated by comparing our proposal with ad-hoc case-by-case implementations of regulatory compliance and by using execution indicators related to the overhead of the SIP, iii) the appropriateness to relevant application domains, notably e-government and e-health, which will be evaluated by applying the mechanisms to mainstream regulations.

On another hand, the main differences between our work and other existing proposals on regulatory compliance in service-based systems are: i) the focus on inter-organizational contexts, which is an open research area addressed by ongoing projects [14], (ii) the proposal of enforcement mechanisms and not only monitoring ones, iii) the formal specification of the integration platform using Event-B, iv) leveraging the capabilities of middleware technologies as first-class citizens to build the solutions.

8 Conclusions and Future Work

This work proposes solutions, at different abstraction levels, to monitor and enforce compliance requirements within inter-organizational SIPs. The solutions leverage well-known EIP and specialized capabilities of SIPs which are then mapped to specific middleware technologies (e.g. ESB). The proposed methodology aims at incrementally addressing the main issues by identifying the required capabilities as well as specifying and prototyping the proposed solutions in order to evaluate them.

Future work in this research line will include the detailed design of the proposed platform and a formal specification using Event-B. We will also address the identification and specification of relevant compliance requirements in selected application domains (e-government and e-health). Finally, it will also include developing prototypes to evaluate the proposed solutions. In the long term, future work will address other application domains and other types of requirements as well as using different middleware technologies and products to implement prototypes. Finally, this work will be a step forward on discussing strategies to efficiently implement regulatory compliance mechanisms in e-government taking advantage of existing platforms.

References

1. Di Nitto, E., Ghezzi, C., Metzger, A., Papazoglou, M., Pohl, K.: A journey to highly dynamic, self-adaptive service-based applications. Autom. Softw. Eng. 15, 313–341 (2008)
2. De Michelis, G., Dubois, E., Jarke, M., Matthes, F., Mylopoulos, J., Papazoglou, P., Pohl, K., Schmidt, J.W., Woo, C., Yu, E.: Cooperative information systems: a manifesto. Citeseer (1996)
3. Mylopoulos, J.: Cooperative Information Systems. IEEE Expert 12, 28–31 (1997)
4. Mecella, M., Scannapieco, M., Virgillito, A., Baldoni, R., Catarci, T., Batini, C.: Managing Data Quality in Cooperative Information Systems. On the Move to Meaningful Internet Systems. Springer, London (2002)
5. Call for Papers of the 22th International Conference on Cooperative Information Systems, CoopIS 2014 (2014), `http://www.onthemove-conferences.org/index.php/coopis14`
6. González, L., Ruggia, R., Abin, J., Llambías, G., Sosa, R., Rienzi, B., Bello, D., Álvarez, F.: A service-oriented integration platform to support a joined-up E-government approach: The uruguayan experience. In: Kő, A., Leitner, C., Leitold, H., Prosser, A. (eds.) EDEM 2012 and EGOVIS 2012. LNCS, vol. 7452, pp. 140–154. Springer, Heidelberg (2012)
7. Baru, C., Botts, N., Horan, T., Patrick, K., Feldman, S.S.: A Seeded Cloud Approach to Health Cyberinfrastructure: Preliminary Architecture Design and Case Applications. In: 2012 45th Hawaii International Conference on System Science (HICSS). IEEE (2012)
8. Pezzini, M., Lheureux, B.J.: Integration Platform as a Service: Moving Integration to the Cloud. Gartner (2011)
9. Ferguson, D.: The internet service bus. Move Meaningful Internet Syst. In: 2007 CoopIS DOA ODBASE GADA IS., p. 5 (2010)
10. Peter Mell, Timothy Grance: The NIST Definition of Cloud Computing. NIST
11. Papazoglou, M.P.: Making Business Processes Compliant to Standards and Regulations. In: Enterprise Distributed Object Computing Conference, EDOC (2011)

12. Turetken, O., Elgammal, A., van den Heuvel, W.-J., Papazoglou, M.: Enforcing Compliance on Business Processes through the use of Patterns (2011)
13. Knuplesch, D., Reichert, M., Mangler, J., Rinderle-Ma, S., Fdhila, W.: Towards compliance of cross-organizational processes and their changes. In: La Rosa, M., Soffer, P. (eds.) BPM Workshops 2012. LNBIP, vol. 132, pp. 649–661. Springer, Heidelberg (2013)
14. Knuplesch, D., Reichert, M., Fdhila, W., Rinderle-Ma, S.: On enabling compliance of cross-organizational business processes. In: Daniel, F., Wang, J., Weber, B. (eds.) BPM 2013. LNCS, vol. 8094, pp. 146–154. Springer, Heidelberg (2013)
15. COMPAS: COMPAS Project - Final Report (2011)
16. Birukou, A., D'Andrea, V., Leymann, F., Serafinski, J., Silveira, P., Strauch, S., Tluczek, M.: An integrated solution for runtime compliance governance in SOA. In: Maglio, P.P., Weske, M., Yang, J., Fantinato, M. (eds.) ICSOC 2010. LNCS, vol. 6470, pp. 122–136. Springer, Heidelberg (2010)
17. Holmes, T., Mulo, E., Zdun, U., Dustdar, S.: Model-aware Monitoring of SOAs for Compliance. Service Engineering, pp. 117–136. Springer, Vienna (2011)
18. Koetter, F., Kochanowski, M.: A model-driven approach for event-based business process monitoring. In: La Rosa, M., Soffer, P. (eds.) BPM Workshops 2012. Lecture Notes in Business Information Processing, vol. 132, pp. 378–389. Springer, Heidelberg (2013)
19. Weidlich, M., Ziekow, H., Mendling, J., Günther, O., Weske, M., Desai, N.: Event-Based Monitoring of Process Execution Violations. In: Rinderle-Ma, S., Toumani, F., Wolf, K. (eds.) BPM 2011. LNCS, vol. 6896, pp. 182–198. Springer, Heidelberg (2011)
20. Ben Hamida, A., Bertolino, A., Calabrò, A., De Angelis, G., Lago, N., Lesbegueries, J.: Monitoring Service Choreographies from Multiple Sources. In: Avgeriou, P. (ed.) SERENE 2012. LNCS, vol. 7527, pp. 134–149. Springer, Heidelberg (2012)
21. Baouab, A., Perrin, O., Godart, C.: An Event-Driven Approach for Runtime Verification of Inter-organizational Choreographies. In: International Conference on Services Computing (2011)
22. Armellin, G., Betti, D., Casati, F., Chiasera, A., Martinez, G., Stevovic, J.: Privacy preserving event driven integration for interoperating social and health systems. In: Jonker, W., Petković, M. (eds.) SDM 2010. LNCS, vol. 6358, pp. 54–69. Springer, Heidelberg (2010)
23. Wylie, H., Lambros, P.: Enterprise Connectivity Patterns: Implementing integration solutions with IBM's Enterprise Service Bus products
24. Hohpe, G., Woolf, B.: Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions. Addison-Wesley Professional (2003)
25. González, L., Ruggia, R.: Adaptive ESB Infrastructure for SBS. Adaptive Web Services for Modular and Reusable Software Development: Tactics and Solutions. IGI Global (2012)
26. González, L., Ortiz, G.: An ESB-Based Infrastructure for Event-Driven Context-Aware Web Services. In: Canal, C., Villari, M. (eds.) ESOCC 2013. CCIS, vol. 393, pp. 360–369. Springer, Heidelberg (2013)
27. Riezi, B., González, L., Ruggia, R.: Towards an ESB-Based Enterprise Integration Platform for Geospatial Web Services. In: The Fifth International Conference on Advanced Geographic Information Systems, Applications, and Services, Nice, France (2013)
28. Llambías, G., Ruggia, R.: A middleware-based platform for the integration of Bioinformatic services. XL Conferencia Latinoamericana en Informática, Uruguay (2014)
29. Abrial, J.-R.: Modeling in Event-B: System and Software Engineering. Cambridge University Press, Cambridge (2010)
30. Tounsi, I., Hadj Kacem, M., Hadj Kacem, A.: Building correct by construction SOA design patterns: Modeling and refinement. In: Drira, K. (ed.) ECSA 2013. LNCS, vol. 7957, pp. 33–44. Springer, Heidelberg (2013)
31. González, L., Laborde, J.L., Galnares, M., Fenoglio, M., Ruggia, R.: An adaptive enterprise service bus infrastructure for service based systems. In: Lomuscio, A.R., Nepal, S., Patrizi, F., Benatallah, B., Brandić, I. (eds.) ICSOC 2013. LNCS, vol. 8377, pp. 480–491. Springer, Heidelberg (2014)