

ComCert: Automated Certification of Cloud-based Business Processes

Rafael Accorsi and Lutz Lewis

Department of Telematics
Albert-Ludwigs-Universität Freiburg, Germany
{accorsi,lowis}@iig.uni-freiburg.de

Abstract. A key obstacle to the development of large-scale, reliable Cloud Computing is the difficulty of timely compliance certification of business processes operating in rapidly changing Clouds. Standard audit procedures are hard to conduct for Cloud-based processes. **ComCert** is a novel, well-founded approach to enable automatic compliance certification of business process with regulatory requirements.

Reliable Cloud Computing must provide control over business process compliance. The central task to this end is certifying business processes for their adherence to regulations. However, due to the dynamics of Clouds, current manual audits for compliance certification, such as SAS-70 or SAS-117, are hard to apply in this setting. This is at odds with the increased flexibility that Clouds offer and with which companies can adapt their business processes on demand. Consequently the lack of automated audit methods and the resulting risks of noncompliance [12] currently inhibit enterprises from outsourcing their tasks onto the Cloud and prevent the full realization of the economic potential of Cloud Computing.

ComCert is a method of automated compliance certification of business processes. Intuitively, auditors use ComCert tool support to check Cloud-based processes for adherence to a large set of different compliance requirements. The analysis carried out by ComCert is able to detect vulnerabilities arising from the control-flow and dataflow perspectives, eg, whether all required activities are included and whether activities happen in the prescribed order. If the process is compliant, the approach generates evidence of correctness. If not, it provides counterexamples that identify violations of the compliance policies and indicate the vulnerable spots in the process. In doing so, ComCert complements and extends the research on business process verification, which has traditionally focused on checking the compatibility of communicating processes, ie absence of deadlocks and guarantee of service [14].

ComCert employs Petri nets as a formal basis to decide on the policy adherence of business processes. Petri nets provide an expressive, notation-independent formalism to capture the semantics of business processes. Also, compliance requirements can be expressed as usage control policies [13], and Petri nets serve as formal representation of those policies [9]. Given the Petri net representation of both a process and the applicable policies, the compliance check through ComCert certification is reduced to a type of reachability problem in Petri nets. Put simply, the goal is to demonstrate that the process modelled in one Petri net (the “process net”) satisfies the compliance requirements modelled in another Petri net (the “policy net”). Petri net reachability is a well-investigated problem for which efficient algorithms and, hence, tool support for automation exists.

Since translations from standard process notations such as Business Process Modelling Notation and Business Process Execution Language into Petri nets exist [10], ComCert does not rely on a particular process notation for analysis, thereby being equally suitable for different Cloud-providers in a non-invasive manner. The use of Petri nets for the formalization of compliance requirements allows the circumscription of policy patterns. The refinement from regulations to policies can thus be captured in a formal and unambiguous, yet easily accessible way.

Specifically, ComCert builds upon an extensive classification of compliance requirements drawn from major regulations such as the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act and the PATRIOT Act. The resultant classification consists of three classes, where each requirement either (1) requires certain activities to (not) be performed before or after other activities, (2) describes the mandatory flow of data between activities and (3) prescribes additional conditions on data, eg pseudonymization and retention. Petri nets formalize these classes as high-level patterns, thereby reducing the effort for the specification of requirements. For a particular application domain and regulation, concrete requirements are stepwise refined into instances of high-level patterns. With instantiated patterns, it is also possible to detect policy inconsistencies in an automated manner. If the policy nets contradict each other, the conflicts are flagged, eg, if a regulation requires the retention of data while a competing regulation demands its deletion.

It is important to note that the compliance certificates regard only the process model and not the organizational [8] and technical layers [1–3]. General policies such as creating backups and logs, securing the network, raising the workforce’s security awareness or having a security manage-

ment process with risk assessments are an integral part of security efforts, but they do not pertain to a specific process model. Regarding the certification of the system components and procedures, for example, the execution engine and virtualization issues, additional vulnerability analysis [11] and standard procedures as from COBIT and ISO 17799 would need to be considered.

Case studies using ComCert show that the “push-button” compliance check is feasible for industrial business processes. Ongoing investigation focuses on extending the kinds of analysis that can be carried out with ComCert. In particular, we are experimenting with information flow analysis and control techniques for Petri nets to detect interferences between communicating processes [4–7]. These interferences denote further, more subtle but equally threatening design vulnerabilities that have not yet been considered in the certification of Cloud-based business processes.

Taking stock, ComCert contributes to automating the compliance certification of processes in the Cloud and consequently, fosters wider Cloud deployment and the compliant implementation of Cloud-based business models.

Link

<http://www.telematik.uni-freiburg.de/comcert>

References

1. R. Accorsi. *Automated Counterexample-Driven Audits of Authentic System Records*. PhD thesis, University of Freiburg, 2008.
2. R. Accorsi. Automated privacy audits to complement the notion of control for identity management. In E. de Leeuw, S. Fischer-Hübner, J. Tseng, and J. Borking, editors, *Policies and Research in Identity Management*, volume 261 of *IFIP Conference Proceedings*, pages 39–48. Springer, 2008.
3. R. Accorsi and T. Stocker. Automated privacy audits based on pruning of log data. In *Proceedings of the EDOC International Workshop on Security and Privacy in Enterprise Computing*. IEEE, 2008.
4. R. Accorsi and C. Wonnemann. Detective information flow analysis for business processes. In W. Abramowicz, L. Macaszek, R. Kowalczyk, and A. Speck, editors, *Business Processes, Services Computing and Intelligent Service Management*, volume 147 of *Lecture Notes in Informatics*, pages 223–224. Springer, 2009.
5. R. Accorsi and C. Wonnemann. Auditing workflow executions against dataflow policies. In W. Abramowicz and R. Tolksdorf, editors, *Proceedings of the Business Information Systems*, volume 47 of *Lecture Notes in Business Information Processing*, pages 207–217. Springer, 2010.
6. R. Accorsi and C. Wonnemann. Information flow analysis of business processes for confidentiality requirements. In *To appear in the Proceedings of the Workshop*

- on Security and Trust Management*, Lecture Notes in Computer Science. Springer, 2010.
7. R. Accorsi and C. Wonnemann. Static information flow analysis of workflow models. In *To appear in the Proceedings of the Conference on Business Process and Service Computing*, Lecture Notes in Informatics. Springer, 2010.
 8. A. Carlin and F. Gallegos. IT audit: A critical business process. *IEEE Computer*, 40(7):87–89, July 2007.
 9. H. Huang and H. Kirchner. Component-based security policy design with colored petri nets. In J. Palsberg, editor, *Semantics and Algebraic Specification*, volume 5700 of *Lecture Notes in Computer Science*, pages 21–42. Springer, 2009.
 10. N. Lohmann, E. Verbeek, and R. Dijkman. Petri net transformations for business processes - A survey. In K. Jensen and W. van der Aalst, editors, *Transactions on Petri Nets and Other Models of Concurrency*, volume 5460 of *Lecture Notes in Computer Science*, pages 46–63. Springer, 2009.
 11. L. Lewis and R. Accorsi. Finding vulnerabilities in SOA-based business processes. *IEEE Transactions on Service Computing*, 2010. To appear.
 12. G. Müller, R. Accorsi, S. Höhn, and S. Sackmann. Sichere Nutzungskontrolle für mehr Transparenz in Finanzmärkten. *Informatik Spektrum*, 33(1):3–13, February 2010.
 13. S. Sackmann and M. Kähler. ExpPDT: A policy-based approach for automating compliance. *Wirtschaftsinformatik*, 50(5):366–374, October 2008.
 14. W. M. P. van der Aalst and A. H. M. ter Hofstede. Verification of workflow task structures: A petri-net-based approach. *Information Systems*, 25(1):43–69, 2000.