

Preface

For a number of years now, Web Services Business Process Execution Language (WS-BPEL or BPEL for short) is broadly used for the definition of executable business processes. By exploiting the fact that BPEL is a platform-independent standard supported by several major vendors of business suites, business processes specified with BPEL may be developed at one site and afterwards be executed at other sites without any further transformation. In this manner, business processes spanning organisational boundaries can be specified or modified at a central site and (re)distributed to the enterprises involved for execution in order to serve a common goal.

Such an approach of centralised definition seems to be particularly useful in scenarios where the need of comparatively small modifications of existing local processes to adapt to changing overall requirements occurs frequently and the requirement changes mainly are caused by one of the partners involved. Supply chain management is an example of such a scenario where typically processes of different suppliers have to be coordinated to serve one manufacturer's needs.

In such scenarios, considerable amount of coordination effort could be avoided by central modification and adaptation of the distributed processes. However, concerns that a remotely defined business process could possibly fail to conform to local security policies or, more generally, local business rules often stand in the way of these potential savings. In particular, worry is dedicated to the risk that a business process defined at a site outside the own enterprise and executed on behalf of this external site would fail to obey the restrictions of information and control flows induced by local security policies, may it occur because of insufficient knowledge or because of intentional disregard of such restrictions.

A local process defined as part of an overall process may need access to protected information or resources that, conforming to local security policies, must not be granted to any site outside the own enterprise. Since such local processes typically communicate with other parts of the overall process, such access will only be granted to the local process if it can be made sure that the protected information will not be disclosed across enterprise boundaries and protected resources will only be used within the limits prescribed by security policies.

Checking a process definition for compliance to constraints of information and control flows, ideally prior to execution of the process, is generally considered a demanding task that may easily require more effort than could have been saved by avoiding coordination overhead. This might be the reason why such exploitation of the capability for platform-independent definition of business processes in order to

reduce adaptation effort with business processes spanning enterprise boundaries often will not even be envisaged.

In the application layer, security policy enforcement at runtime often is performed by exertion of role-based access control (RBAC). Conforming to the underlying principles of RBAC to safeguard confidentiality and integrity, a business process communicating with sites outside the own enterprise, in general, would not be granted access to protected information or resources. Reason for this is that for the decision to grant access RBAC usually does not take into account the disposition of information provided in the further course of action within the process requesting access. Thus, security policy enforcement at runtime using RBAC offers no alternative to complex analysis of business processes with respect to compliance to security policies prior to execution since RBAC would have to prevent courses of action in enterprise-spanning business processes that are reasonable and required in the context of the overall process.

Hence, we are facing the following dilemma: On one hand side, there is the opportunity to save a considerable amount of effort required for development and adaptation of business processes by exploiting the property of BPEL being a platform-independent standard for the definition of executable business processes. On the other hand side, this opportunity either cannot be made use of because of security concerns or the effort possibly saved has to be spent otherwise for checking compliance to security policies in order to dispel such security concerns.

In this book based on the author's research, methods and procedures will be introduced that help to resolve this dilemma. These procedures allow for performing the required check of compliance to security policies prior to execution of a business process in a comparatively easy way. Even more, the procedures to analyse BPEL scripts defining business processes are suited to be performed automatically such that they can be checked quickly and with little effort. This, of course, is of great value in security policy compliance assessment of remotely-defined business processes in enterprise-spanning scenarios. Furthermore, this approach may also be applied beneficially to save effort in quality assurance when assessing compliance to security policies of business processes that have been developed within an organisation for internal use only.

Finally, the procedures developed for the field of organisation-spanning business processes will be generalised in such a way that they also become applicable with Grid and Cloud computing.

Dr. Klaus-Peter Fischer-Hellmann

June 2012

Information Flow Based Security Control Beyond RBAC
How to enable fine-grained security policy enforcement
in business processes beyond limitations of role-based
access control (RBAC)

Fischer-Hellmann, K.-P. - Bischoff, R. (Ed.)

2012, XXI, 161 p. 25 illus., Softcover

ISBN: 978-3-8348-2617-6