Compliance and Privacy in Enterprise SOA Ecosystem

Jean-Christophe Pazzaglia
SAP Research – Security & Trust

Position statement for the W3C Workshop on
Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement
Draft

Traditionally, organizations develop custom applications from scratch and use various platforms, but then find that they lack the flexibility to accommodate change. Moving from core (focusing on Invention and Innovation) to context (focus on productivity, standardization and commoditization, in order to consolidate common IT practices), but rather, for example, is difficult and expensive. To make the move, enterprises must analyze their IT landscape to determine which assets to replace, upgrade, or make obsolete; acquire new skills; and support integration with new applications. Conversely, developing innovative processes from the context into the core is equally challenging and expensive.

- **The question:** How can organizations in such a situation act effectively while complying with global and local regulations?
- **The answer:** Not easily. Many organizations look for better ways to centralize common functions as shared services, rid themselves of redundancy, increase their operating efficiency, and enable reuse of their existing investments. Unfortunately, the growing complexity of the organization's IT landscape often hampers these laudable goals.

Among other compliance requirements, protecting the individual's privacy on the Internet is crucial to the future of Internet-based business and the move toward a true Internet economy. SAP firmly commits to secure and trustworthy Internet commerce and the individual's right to privacy.

For example, in order to grant access to our public Web site, we ask the user's consent to the collection and use of the information. If we decide to make changes to the privacy policy, we post the changes so that the user will always know what information will be collected, and how we use it. Today, our privacy policy focuses on raising user awareness on data usage while, complementary we provide the necessary security measures to enforce it.

- **Use and Purpose of Collected Personal Data**
  On our Web sites, we only store personal information relating to users with their permissions. The user may choose to reveal information to us if, for example, he registers or completes a survey. Companies in the SAP group may use the information internationally in connection with processing the inquiries and orders or to help improve our products and services.
  We would only share such information with third parties outside the SAP group with the user's express permission or as required by the applicable law. Information is used solely for the purposes described below.

- **Privacy Across the Entire SAP Network**
  As a global company, SAP operates a number of Web sites around the world. Any information that the user submit to one of our sites in any one country may be sent electronically to a server for one of these sites in another country. We safeguard the user's privacy interests around the world by ensuring that this SAP site adheres to our international data-protection principles described in this statement.
  We bind our employees to observe privacy and confidentiality rights.

- **Online Security**
  SAP supports secure online shopping using secure server technology because we want the shopping experience to be simple and safe. There are state-of-the art security arrangements and facilities on SAP sites to prevent security abuse.

SAP Research is investigating how the evolution of IT solutions, and notably the emergence of Enterprise SOA, will impact the current IT Security Governance model. More precisely, we are willing to investigate the models and mechanisms that should be used to express, negotiate and enforce different legal requirements such as privacy in the context of a complex and dynamic collaboration of Enterprise services spanning across different trust domains. Our vision is that we should:

- Develop methodological and development support to systematically achieve security applications composed of services and utilising dedicated security and dependability services guidelines, templates, languages, logics, tools and frameworks
- Establish the foundations of a secure service infrastructure spanning corporations, nations and societies need for governmental and societal control and the accompanying legal framework
- Invest research into trusted infrastructure which extend and strengthen the range of security properties that can be enforced independently of higher level services
- Find appropriate models and abstractions to reason about the economics, and predictability of system wide security and dependability properties.
- Understand how current IT Security Governance models can or should evolve into appropriate SOA Security Governance.

Being able to express privacy policies, to achieve negotiation across domains and to control that these policies are correctly enforced is clearly an element of this global picture.