W3C Workshop on
Rule Languages
for Interoperability

27-28 April 2005 — Washington, D.C.

Call for Papers Submission

Abstract: This paper is submitted to focus on the need for rule languages to establish and maintain a high level of expressiveness, sufficient to facilitate the governance of organizations and relationships. The vision of the Semantic Web embraces the capacity for rule languages to express, and bind actors to, policy-based rules (including legal requirements) that are to be performed by systems and services. Two important areas in which the development of interoperable, expressive rule languages should be developed include rulebases for assuring the reliability of corporate information and expressing the security of software code applications (in order to document the adherence of those applications to the expressed rules).

Statement of Issues: Recent attention to compliance functions within corporate enterprises has emphasized the importance of structuring and operating systems-based controls to achieve certain legal requirements. The attention to using IT systems for achieving policy objectives has brought into focus the importance of having available a variety of mechanisms through which compliance obligations can be expressed.

It is important to underscore that virtually any business, particularly small to medium enterprises that are dependent on the Web for their economic viability, is impacted. While much of the compliance attention has been given to large companies, those companies have, in turn, entered into contracts with smaller businesses as service providers; the contracts impose upon the service providers the duty to align their services to various policy-based requirements as conditions for doing business. But traditional contracts are no longer adequate to express the detail and richness of the rules to be implemented.

This paper proposes that the activities of the rules community (and any possible W3C Working Group) should take into account that the rules languages to be developed must be sufficiently flexible to permit businesses to take advantage of the platform provided by the Web for interchanges and interoperability and incorporate code-based expressions of their policy requirements. Stated differently, *business rule languages should be developed and endorsed which permit expression of the requirements of law in programmable code*.

In the current business environment, two of the most difficult aspects of implementing commercial services that include Web-based delivery arise from the challenge of expressing the binding requirements relating to the following:

- Information Security Controls: As two parties exchange data, or one party provides processing services for another, it has become essential that information security controls be defined and imposed by contract on the relationship. Many of the specific controls originate from external legal requirements (such as US laws such as Sarbanes-Oxley, HIPAA, Gramm-Leach Bliley and similar legal materials). Doing so is very difficult, since neither lawyers nor businesses have available (within the typical written contract) the tools used by IT professionals and systems to express information security controls. As a result, contracts become more complicated, and run the risk of omitting or improperly expressing the suitable requirements. In most instances, the contracts are simply proving insufficient at communicating all of the applicable business rules.

- Software Vulnerabilities: With the recognition that many security risks are associated with the exploitation of vulnerabilities in software code, many users have been increasingly vigilant in wishing to express requirements regarding the manner in which software design and development occurs. As best exemplified by the CMU CMMI® methodology, many of the requirements associate with system-based controls.

  The user community is also experiencing regulatory oversight of internal development processes, in order to better assure that the software code developed internally (as compared to being acquired from licensors) similar meets quality controls. There is an urgent need for code offered to perform services (including Web services) to be able to demonstrate its suitability against the policy-based requirements relating to improved software design expectations.

Based on the preceding, I propose that the result of rules language development should *include the capacity to express legal requirements in programmable code.* Achieving this result can, by example, advance two important objectives for any company:

- better assure the reliability of financial information (through the expression of information security controls); and
- prevent the development or acquisition of software code that contains vulnerabilities.

Accordingly, two examples of rulebases that should be prioritized as policy-based rules would be the following:

- *Information Security Controls*--Rules that express information security controls, to be employed by service providers or supply chain participants, necessary to assure the reliability of financial data produced through the services/supply chain functions (i.e., expression of COBIT or ISO 17799 requirements).

- *Vulnerability Testing*--Rules that express requirements, and permit validation, for assuring that software code has been verified against published vulnerability lists or otherwise investigated for the absence of known vulnerabilities that can be exploited by malicious actors.

Rationale:

Information Security Controls: Companies that have executed Sarbanes-Oxley compliance programs realize that ongoing corporate investments will be required; those investments must balance difficult aspects of modern business:

- First, companies must develop and assure internal compliance with the business rules that reflect controls designed to manage recognized risks that place in jeopardy the integrity of financial information.

- Second, companies must convey to their service providers and supply chain partners (both upstream and downstream), often as part of complex contractual relationships, requirements that extend their internal compliance rules onto the third parties and require adherence to those rules as a part of the business relationship.

Many companies that are not SEC-regulated entities, but who act as service providers or suppliers to those entities, have discovered that they must execute divergent and often poorly expressed business rules for accomplishing identical business functions for assuring the reliability and security of business data. This has created significant hardships, particularly since mature, strong standards (such as COBIT or ISO 17799) have been employed by many SEC-regulated entities as the foundation for their Sarbanes-Oxley compliance programs.

Standardized, interoperable business rules would permit regulated companies to both a) achieve greater internal efficiency in aligning program and data-specific controls to higher-level policy requirements and b) communicating, implementing, auditing and enforcing the use of those or related controls by their service providers and supply chain partners.

Vulnerability Testing—Increasingly, both internal development operations and third-party software is under scrutiny in order to assure that the resulting code does not reflect

known vulnerabilities that can be the means by which malicious actors can intrude upon, or otherwise disrupt, production data or the related information systems. However, despite significant progress in identifying various vulnerabilities (and developing diagnostic tools and processes for detecting the existence of those vulnerabilities), companies face increasingly significant barriers in how to integrate those tools into development activities, while also producing certification or other audit results which serve to validate that known vulnerabilities do not exist with respect to specific target assets or programs.

Development of a rules library which would permit code assets to be tested uniformly for vulnerabilities would also promote a greater awareness for the objectives and values of interoperable rule languages and their by-products.

A significant benefit of this focus will be to facilitate improved confidence in the code assets used within web services and other applications that will implement the Semantic Web vision. By providing auditable data (produced through rule-based mechanisms) that code is itself produced in a secure manner, significant improvements can be achieved in accelerating the ease with which business processes can be outsourced or delegated to web-services.

Submitter:

This paper is submitted by Jeffrey B. Ritter. Mr. Ritter currently practices law, assisting clients in contractual implementations of information security controls and the production of compliance systems for various regulatory environments, both domestically within the United States and in Europe. Mr. Ritter has nearly 15 years experience in standards development activities, having previously served as a Co-Rapporteur to UN/CEFACT (EDIFACT standards) and various trade association/standards bodies. He also has contributed to the development of various model legal environments (contracts, statutes, conventions) for standards-based data transactions. This submission represents his personal views and is not the expression of the views of the law firm at which he is a partner, Kirkpatrick & Lockhart Nicholson Graham LLP, or any of his or their clients. He may be reached at 202.285.7385, jeffrey.ritter@comcast.net.