

To the Identity Industry – An Open Call for Role Interoperability Standards

As the chief technology officer of SailPoint Technologies, I work closely with customers and partners who are tackling the complex issues of governance, risk, and compliance around identity management. Many customers and vendors (including SailPoint) are implementing role-based access control (RBAC) as a component of the solutions designed to address these requirements. Without a doubt, RBAC provides a valuable framework for controlling users' access to information and for reducing risks and meeting identity compliance and governance requirements.

Interestingly, though, as RBAC models become more prevalent in the runtime identity and security infrastructure, more and more companies are encountering a technical barrier to successful deployment – the lack of a standards-based way to define the sharing and interoperability of RBAC models between different identity-aware systems.

Realistically, there will never be a single, monolithic role model across a large organization.

Roles and role models exist – and will continue to exist – in multiple products like access control, provisioning, network access, and of course in enterprise role management solutions. Given this reality, in order for roles to be a truly valid visibility and control vehicle for identity governance, we have to understand how roles and role models interrelate, and we must be able to describe and exchange them in an open, standards-based way.

A Technical View of the Problem

Identity-aware systems, such as enterprise provisioning, centralized access control, privileged user management and content management systems, frequently share an identity context through the use of common identity repositories, but they rarely (if ever) share a common physical role model store. Most, if not all, enterprise applications that employ an RBAC model do so as autonomously operating entities. Each independent system runs its own individual role model and there is no standards-based way for those systems to share, exchange or publish that model to master, peer or subordinate systems. Even if these isolated RBAC systems do share elements of their role models for runtime access control decisions, they do not share a true “operational context” for the model itself.

Today, there is no overarching operational control standard that includes role model definition and delegated change control, functional and operational methods, role and target system mapping, and the expression of a shared state model for the role definition itself.

As complex RBAC models span the boundaries of identity-aware systems, this operational context becomes just as important as the model definition. Defining, enforcing and maintaining the various usage rules required to promote and maintain identity governance requires the definition of a new standards-based approach to RBAC control directives. Existing role management standards address *some* of the issues around role interoperability, but none provides a *complete* solution that includes the operational context. The recent work of the INCITS CS1.1 sub committee on operational and functional exchange, and the work of the OASIS XACML Technical Committee on its RBAC profile, both present strong foundational groundwork

for the proposed effort. These existing specifications need to be brought together, extended and enhanced to create a complete control framework for shared role models.

Call to Action

As an identity and access management community, I believe it's our responsibility to create a complete operational exchange model for roles. That's why, today, I am inviting the identity development community and its thought leaders to join me to collaborate on a standard for role interoperability and exchange.

To help organize and promote this effort, I have created an information portal and discussion forum at www.openroleexchange.org. On the site you can contribute to an open discussion group and download a white paper that discusses the subject of open role exchange in more detail. I will also be attending the Burton Catalyst conference next week in San Diego, and welcome the opportunity to discuss this proposal in-person.

The Open Role Exchange Forum will host an interactive webinar on July 16th at 1 p.m. CDT to further discuss this topic and relay up to date information on this proposal. To register for this event, please go to the open role exchange website at www.openroleexchange.org.

In conclusion, the goal of this initiative is to bring the identity management community together to define role interoperability standards that will solve difficult integration problems and simplify role-based governance across diverse identity systems. I believe that role interoperability standards will benefit our industry as a whole and will allow technology vendors to focus on bringing to market new solutions that meet the growing need for governance, risk and role-based control for identity.

I look forward to a lively discussion and measurable progress over the coming months.

Sincerely,

A handwritten signature in black ink, appearing to read "D. J. Rolls". The signature is stylized and somewhat cursive, with the letters "D", "J", and "R" being the most prominent.

Darran Rolls,
Chief Technology Officer, SailPoint Technologies
darran.rolls@sailpoint.com