**Authentication, federation, and SSO**

The federation concept is familiar inside the firewall, perhaps best exemplified by the ubiquitous Microsoft Windows domain model. Enterprises can link multiple Windows domains by defining the trust model between different organizations within the firewall and allowing authentication to be delegated to the “local” domain and trusted by a remote domain using Kerberos, making login transparent to the end user.

Modern federation takes this model beyond the pro­prietary Microsoft approach to make seamless SSO work across the Internet using SAML, an XML-based open stan­dard for exchanging authentication and authorization data between security domains - that is, between an identity provider and a service provider - instead of Kerberos.

The problem with federation and SSO is that, after more than a decade, SAML adoption has not risen above 10 percent of enterprise apps - apparently due to the exces­sive costs of infrastructure software. There simply is not enough return on investment for most service providers to implement, expand, and manage a complex federation network. The industry must therefore go beyond SAML and focus on the core HTTP authentication standard. It requires no change to the target app and no coordination between users and the application. HTTP is the gold stan­dard in authentication, with nearly 100 percent of Web apps supporting it.