LETTER FROM THE GUEST CONTENT EDITOR

I am honored and humbled to have been asked to guest edit this issue of Information Standards Quarterly on Identity Management. I have been involved in the evolution and application of identity standards for many years and am thrilled to have been able to bring authors from very different disciplines together to contribute to this issue. I hope you find this as informative, insightful, and entertaining as I do.

The same way as Bring Your Own Device (BYOD) has been reshaping the face of institutional computing, Bring Your Own Identity (BYOI) will be equally impactful. It is probable that BYOI may even help us overcome some of the unresolved issues of BYOD. Devices are often used as a proxy for Identity but they are a poor proxy at best. The articles in this issue start to show how the emerging identity management standards can be leveraged to solve long-standing problems.

Dan Blum’s piece on Privacy by Design establishes some of the core patterns for applying the latest standards to build systems that leverage the new standards. Dan introduces concrete ways that systems can be designed and built that solve existing problems while increasing personal privacy, assurance, and control.

Don Hamparian gives us a glimpse into what is happening at OCLC, an organization enabling controlled access to licensed content on a global scale. OCLC is a true leader in this space having built a SAML-based federation with 23,000 institutional partners acting as Identity Providers. Don’s work at OCLC is a great example of what can be done today bringing these standards together with a strong institutional desire to engage with end users in a respectful and privacy-protecting way.

Doc Searls, one of the thought leaders in the identity standards space paints a picture of a world where the emerging standards have become commonplace. Doc’s vision helped create the bi-annual Internet Identity Workshop (IIW), the conference where the cutting edge of internet identity innovation is formed. Doc has also been one of the primary shepherds for the advancement of Vendor Relationship Management (VRM), a user-centric alternative to Customer Relationship Management (CRM).

Finally, Mike Jones’s piece introduces us to the richness of the JSON-based identity protocol suite that has evolved from protocols such as OpenID and OAuth. While these protocols originated in and emerged from the social networking space they have been rapidly adopted (for standards (©). They have evolved to support a wider range of use cases with higher levels of assurance and can support transactions of higher value and regulatory compliance needs.

It may seem remiss not to mention the SAML-based protocol stack1 in an issue about identity management. We decided that rather than repeating recently covered territory we would refer you to the NISO Establishing Suggested Practices Regarding Single Sign-On (ESPReSSO)2 recommended practice, which has been covered previously in this publication (see also inside front cover in this issue). SAML and the Shibboleth3 implementation of SAML are widely adopted in institutional identity management.

Interestingly, leading commercial products such as Microsoft’s Azure Active Directory and Ping Identity’s Ping Federate product have been extending their support for the JSON-based identity protocol suite alongside their support for SAML.

I hope that a journey through this issue of ISQ will leave you not only better informed about the standards that are evolving in the Identity Management space but also help you understand the intention behind those standards and the promise that they represent. doi: 10.3789/isqv26no3.2014.01

All the best,

Andy Dale | CTO of Respect Network Corp.

1 SAML. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
2 ESPReSSO. http://www.niso.org/workrooms/sso
4 Shibboleth. https://shibboleth.net/