Testimony to the HITSC PSWG Public Hearing
Eve Maler, Forrester Research
Submitted March 6, 2014

Following is testimony on NSTIC Ecosystem and Identity Management Standards from Eve Maler of Forrester Research. Some biographical information:

Eve Maler is a principal analyst at Forrester Research, Inc. serving Security & Risk Professionals. She is an expert on emerging identity and security solutions, identity federation, consumer-facing identity and web access management, distributed authorization, privacy enhancement, and API security. Eve has been designated a Privacy By Design Ambassador. Eve founded and runs the User-Managed Access (UMA) standards effort. Prior to joining Forrester, Eve was an identity solutions architect with PayPal, developing business and technical strategies for new consumer identity services offerings. Previously, Eve managed Sun Microsystems' technical collaborations with Microsoft on web services and federated identity interoperability, and she made major leadership, technical, and education contributions to the development of the SAML standard for federated identity. Eve holds a B.A. in linguistics from Brandeis University.

What standards are being looked at to support NSTIC (such as SAML, OAUTH, OpenID connect, PKI), and what are the standards on the periphery (such as XACML)?

Forrester tracks open standards related to identity and access management (IAM) and their overall value to businesses, including with respect to consumer-facing online systems, a key focus for NSTIC. For the purposes of this research, we have defined "open standard" as:

Must involve only openly specified and openly usable protocols, formats, and mechanisms. The maintainers of the specifications must not charge for access to the specifications, nor charge license fees for using any intellectual property therein.

Following are the key standards we are tracking that have relevance to NSTIC's scope and purpose, along with brief assessments of their overall value to businesses and to NSTIC. Note that we are also tracking a number of other standards that generally have only enterprise-facing value; we have not included those here. The phase names used below have the following definitions:

Forrester divides technology ecosystem maturity into five sequential phases. Technologies move naturally through five distinct stages: 1) Creation in labs and early pilot projects; 2) Survival in the market; 3) Growth as adoption starts to take off; 4) Equilibrium from the installed base; and 5) Decline into obsolescence as other technologies take their place.

Standard	Success trajectory*	Phase*	Benefits	Challenges	NSTIC value
BrowserID	Minimal	Survival	Mozilla-supported	Email- and browser-based, low adoption	Low
CAS	Minimal	Equilibrium	Higher ed-friendly	Limited functionality	Low
JWT	Significant	Growth	Mobile/API-friendly identity assertions	Emerging tech	High and central
OAuth	Significant	Growth	Mobile/API-friendly web services security	Emerging tech	High and central
OpenID	Minimal	Decline	Simple SSO tech	Limited functionality, weak security	Low
OpenID Connect	Significant	Growth	Mobile/API-friendly SSO	Emerging tech	High and central
SAML	Moderate	Growth	Enterprise-friendly web SSO	Heavy for mobile/API use and limited IT resources	Moderate and central
UMA	Significant	Survival	Mobile/API-friendly, proactive user access control, ABAC support	Immature	High and central longer term
X.509	Significant	Growth	Superior security features	Unsuitable for Internet-scale user identity vs. security	Moderate and peripheral
XACML	Moderate	Equilibrium	Comprehensive declarative access policy	Heavy for all use cases	Low and peripheral

* This table's assessments are largely built on ones first published in the October 24, 2012 "TechRadar™ For Security Pros: Zero Trust Identity Standards, Q3 2012" Forrester report. Forrester is currently revising its research in this area, and the assessments here reflect draft updates that may change by publication time.

What standards from NSTIC could be adopted by the healthcare industry? What gaps does NSTIC not cover that the healthcare industry would have to create technology for?

All of the standards that provide value to NSTIC could be applicable to the healthcare industry. Use cases for identity-enabled, patient-empowering, access-controlled healthcare data sharing are technically demanding. They require robust security, as well as properties that enable Internet scaling, agility, and participation by business players that have a lower "IT-savvy" quotient. These needs suggest that the emerging mobile/cloud-friendly technologies can provide particular value.

An area in which we have not yet seen a comprehensive standard emerge is a "personal resource discovery service." This is a problem that both the larger NSTIC effort and the healthcare IT effort share, as exemplified by the "Relationship Location Service" use case submitted to the IDESG. (Blue Button+ has innovated a lightweight partner registry service, which is suggestive of productive approaches to personal discovery.)

Another potential gap is auditability of data access. This has special relevance for broader access control between autonomous parties (as between patient-controlled personal data stores and healthcare providers, or between family members) versus in ordinary single sign-on, where the same person uses applications on both the relying party and identity provider sides. While we have seen healthcare IT standards for "accounting of disclosures," it appears these aren't yet ready for truly loosely coupled Internet systems.

One draft standard with NSTIC value that may be of particular interest to the healthcare industry is UMA, which provides a model for handling and respecting patient consent directives in a highly distributed environment. The communications channels it builds among policy decision points, policy enforcement points, and client applications could provide a basis for higher-order discovery and audit functions.

What other actions may be needed to help accelerate adoption and use of NSTIC in general and specifically within the healthcare realm?

Liability issues have inhibited Internet-scale trusted identity ecosystems. We see consumer-facing "social sign-in" scenarios flower among marketing, news, and eCommerce sites, but we struggle to get broad higher-assurance ecosystems off the ground. Commentators often point to lack of business models as the key problem, but an important underlying issue that weakens business models is liability distribution among loosely coupled partners.

The US credit card industry is planning to roll out a higher-security chip-and-PIN standard in 2015, and faces some of the same challenges as NSTIC. It has innovated a new model nicknamed the "liability shift," which may potentially be instructive in helping remove trust barriers to higher-assurance portable identity. This model enables differential rollout of technology on both the server side (think identity providers) and the client side (think relying parties) of the equation, encouraging a race to the top of

adoption of higher-security systems by placing greater transaction liability on the weaker partner.

What are the existing technologies being applied and/or enhanced? Are there new technologies being developed (as a result of NSTIC)?

The availability and quality of the new crop of emerging technologies, particularly OAuth, OpenID Connect, and JWT, has spurred a vast ecosystem of experimentation and development, including the development of new combinations of flows and assertions. (UMA, based on these same technologies, is starting to see some similar experimentation, for example around "Internet of Things" and higher education scenarios.) Some of the use cases explicitly tackle NSTIC goals.

Though XACML in its current form has shown little of the promise of the emerging standards for solving broad NSTIC challenges, it represents an important solution space, namely, declarative access policy expression and standardized policy evaluation. We see value in putting XACML through a simplification process; an "XACML Lite" with a mobile/cloud design center, not just superficial JSON trappings, would be a valuable addition to the landscape.