Testimony to HIT Standards Committee Privacy & Security Workgroup

John Bradley, Senior Technical Architect, Ping Identity

Mar 12, 2014

Good Morning, thank you for inviting Ping Identity to talk about the National Strategy for Trusted Identities in Cyberspace (NSTIC) progress towards adopting standards that are supported by commercial software venders.

Ping is currently involved in one of the first round pilots, and has participated in other proposals. Ping and other providers are supplying pilot participants with both on premise and cloud based software that support a wide range of protocols.

Almost all of the pilots have OpenID Connect and or OAuth 2 components, and several are using SAML 2 for federated identity. One of the good things about federation between the relying party and the identity provider (IdP) is that it allows innovation around the first mile of authentication.

While NSTIC is not the source of the standards currently deployed in commercial software it is playing an important role in developing use cases and evaluating standards for suitability against the NSTIC principals and the use cases.

Currently the Identity Software venders are seeing the most new activity around the recently approved OpenID Connect and Oauth 2 specifications. Ping's core products introduced support for both of those protocols over a year ago. Currently I don't know of a vender without some level of OAuth 2 support and most with Connect support shipping or in development.

We are aware of work in Health IT around RESTful standards involving HTTPS, OAuth 2 , and OpenID Connect . We are seeing rapid deployment of those protocols outside of health at places like Google, SalesForce and many others.

The GSMA has just created a work group at the OpenID Foundation to create a common profile for all Mobile Network Operators (MNO). This along with social identity providers offering stronger authentication may in the near future provide a large cross section of society with strong interoperable credentials for the first time. This along with appropriate trust frameworks may provide a path to providing patients access to health records.

Within the identity software industry we are aware of FHIR, BB+ and RHEx as applications that rely on the previously mentioned underlying standards. There is certainly work to do in bringing these large systems into production, but many of the building blocks are commercially available now from multiple sources.