Remarks of Catherine Tilton

at the

Hearing on the National Strategy for Trusted Identities in Cyberspace (NSTIC)

held by the

Office of the National Coordinator for Health Information Technology

Health IT Standards Committee

Privacy and Security Workgroup

Date: Wednesday March 12, 2014

Time: 10:00 am to 2:45 pm ET

Location: Virtual Hearing

Good day. My name is Cathy Tilton and I lead Daon's NSTIC pilot, which we called "Advancing Commercial Participation in the NSTIC Ecosystem". Our pilot is funded as a cooperative agreement through NIST and began on 1 October 2012.

Daon's NSTIC pilot employs strong, risk-based, multifactor authentication using a mobile device platform. This technology forms the basis for a new, innovative, identity provider (IDP) service in which relying parties (RPs) can dynamically choose the level of assurance needed for a given transaction and the particular authentication challenges to be issued to the device, including biometric options.

Our pilot intends to investigate 5 primary areas:

1. The suitability of strong, mobile-based authentication technology (including biometrics) for online authentication
2. The willingness of RPs to move to external identity/credential providers and how this fits within their business models
3. The acceptance of subscribers
4. The capability of existing trust frameworks (and certification schemes) to support these scenarios & technology
5. The degree of interoperability achievable

To answer these questions, we planned to align our TrustX™ IDP with existing trust framework standards and NSTIC guiding principles, have this service certified at level of assurance (LoA) 3, and pilot it with 5 cross-sector RPs, while in parallel embarking on a research agenda with our partner Purdue University to assess and identify improvements in the areas of usability, accessibility, security, and privacy.

The most notable relying party participating in our pilot is AARP. AARP's goals for their pilot participation are to:

- Improve their members' online experience
- Facilitate new services requiring higher levels of identity assurance
- Protect member information

- Reduce the number of individual identity credentials required
- Give more control to the individual (member)
- Support family and inter-generational applications
- Investigate usability and user acceptance

In selecting a use case, we first had to identify applications where higher levels of identity assurance were warranted, as many existing AARP member services do not require this. AARP selected as their first use case access to the "AARP Health Record" – a personal health record (PHR) service which is free to all AARP members and which:

- Is an easy-to-use, online tool designed to help people over 50 manage their family health care needs.
- Lets them safely store and access critical health information such as medications, allergies, blood type, immunizations and emergency and provider contact information.
- Lets them print an easy-to-read pocket card with vital stats. They can also quickly access their family's health information from any computer, mobile phone or tablet.
- Helps them prepare for emergencies by allowing them to store their family's health information in one easy-to-access location.

As the information stored in the AARP Health Record can be very personal and sensitive, access to the PHR becomes a "transaction of consequence", warranting higher levels of protection than a password.

At present, we are in the process of integrating the AARP application with the TrustX IDP, with the first phase of the pilot anticipated to "go live" in the June timeframe.

Because we are introducing an innovative solution, we have been "pushing the envelope" in a number of ways that are bound to uncover challenges. We expected to identify gaps in the status quo and we have. Thus, we have no shortage of lessons learned along the way. I'd like to share some of these with you today.

1. The first challenge we ran into involves the identity model itself. Existing trust frameworks were built around a "full function IDP" – that is, one that encompasses the functions of registration authority, identity repository, credential provider/manager, and credential verifier (authentication). However, we found that many RPs have an existing base of subscribers that they already have a relationship with and for whom they possess identity data. They have no need or desire for us to replicate the registration authority function, but are only looking for a strong authentication credential that they could bind to the identity that they held. This aligned well with our existing IdentityX platform capabilities. However, this "credential manager" component service was not certifiable under the existing schemes, even though it was evident that there was a market for it.
    a. As a result, we were forced to build out a full IDP service because we had no guarantee that our component service could be certified.

    b. However, the good news is that the trust frameworks have since moved in this direction and FICAM has issued a new TFPAP that embraces the componentized model.
    c. This also supports a broader marketplace where IDPs can be created from "pre-certified" components (though the IDP itself must still be certified) and service providers can concentrate on their areas of expertise.
2. The second challenge we encountered was that existing standards are not innovation friendly. NIST SP 800-63 is prescriptive in its definition of token types. The concept of "equivalent" or "comparable" methods exists, but the process for determining comparability is undefined. We offer methods that are equivalent to the Multifactor Software Crypto Token; however, the implementation on a mobile device differs from that prescribed in the standard. In a white paper we compared these methods including a comparison of token threats and showed how our method was equivalent or better than the described implementation. Government reviewers agreed; however, because no process for declaring equivalence exists, we were stuck. The only way we could move forward was to submit a change request to SP 800-63, and this is known to be a lengthy process.
    a. We wrote our first paper and began discussions on this issue in February of 2013 and are still in limbo.
3. Related to the above are gaps related to dynamic, risk-based multifactor authentication and biometrics. We ran into the following standards gaps:
    a. SP 800-63 does not recognize biometrics as a token type (even when restricted to a second or third factor) and the SAML Authentication Context option does not include a code for biometrics.
    b. The ability of RPs to dynamically select authentication methods is limited. In some cases, the RP may request an authentication at a specific level of assurance (LoA), which can be mapped to a set of methods, but this restricts the number of combinations available.
    c. Some functions must be performed administratively rather than dynamically; for example, policy management, queries for registered (bound) subscribers, and blocking/unblocking (unbinding) of subscribers.
    d. Authentication requests do not allow for setting of geolocation boundaries.
    e. Transaction descriptions may not be passed to the IDP (for display on the phone). Therefore, these must be administratively set. (This limitation is good for privacy, but not as good for security or troubleshooting.)
    f. Assertions may not contain additional contextual information (such as biometric scores).
    g. Lack of a 'health check' capability (from the RP to the IDP).
4. Another challenge we confronted was FIPS-140 certification of cryptographic modules on mobile devices. Although all four major mobile operating systems – iOS, Android, Blackberry, and Windows – have received FIPS-140 certification, that certification is very specific to the dot release of the operating system and chipset tested – not every possible configuration is on the certified products list. Worse, when a new OS version is released, a certified device instantly becomes an uncertified device. When the mobile device is used as the authentication platform,

the issue becomes apparent. However, these same platforms are used for mobile banking every day!

   a. In SP 800-63 a password or SMS token are given the same level of assurance as a Single-Factor Crypto token (LoA2); however, there are no "certifications" required for these methods.
   b. Commercial entities trust TLS provided within browsers and mobile platforms, it is not unreasonable for this to be acceptable by trust frameworks as well.

5. We also found multiple standards gaps in the areas of sponsorship/binding processes and interfacing to identity proofers/attribute providers.
   a. Existing standards also appear biased towards the issuance of credentials in the form of hard (physical) tokens and secrets.
   b. Standard interfaces and profiles are not targeted to "in-band" applications, which creates problems for RPs developing mobile applications and wanting to incorporate trust framework compliant credentials.
6. Standards do not always consider that someone has to pay, but are more geared towards the "free" model, which may be appropriate for the lower levels of assurance, but not LoA3. Business models need functionality for payment and reconciliation purposes. For example, binding of subscribers has another purpose beyond security – the RP is in effect agreeing to pay for that subscriber to use the credential at their site.
7. We implemented both SAML and OpenID Connect and faced challenges in creating a common user experience for both.
   a. Most notably, OpenID Connect allows the RP to request user attributes on a transaction basis whereas SAML requires this to be done once when the RP-IDP relationship is established.
   b. We also discovered that although OpenID Connect is becoming popular for commercial applications, it is too "bleeding edge" for some RPs, including the government.
8. Lastly, we found that both interoperability and privacy come with a price.
   a. Implementing privacy enhancements can come at the expense of some business processes such as troubleshooting, customer support, life-cycle functions, and payment reconciliation.
   b. Some interesting "predicaments" arise when issuing interoperable credentials such as the case of revocation – what happens when one RP blocks (or unbinds) a subscriber? When and how should this be handled with respect to other RPs who have bound to the same subscriber? If the reason is that the subscriber was found to have falsified their identity or committed fraud, what is the IDPs responsibility? Will the IDP even know the reason?

Time does not permit me to provide a more comprehensive list or additional details, but I am happy to answer your questions during the discussion period

Thank you very much for your attention. I am honored to have been asked to address you.

Speaker Bio

Catherine Tilton is the Daon's project manager for their NSTIC pilot. Daon is a leader in government and commercial identity assurance products, best known for their work in large national ID and border management programs worldwide. Mrs. Tilton is the VP of Standards and Emerging Technologies and has over 30 years of systems engineering and project management experience, including over 20 years in the biometrics and identity management space. She is also a leader in IT standards development, actively participating in ISO, ANSI, INCITS, and OASIS. She currently chairs the Standards Coordination Committee of the Identity Ecosystem Steering Group (IDESG).