Health IT Standards Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

Report to HITSC: Virtual Hearing on the National Strategy for Trusted Identities in Cyberspace (NSTIC)

Hearing held on March 12, 2014
Sponsored by the HITSC Privacy and Security Workgroup (PSWG)

Dixie Baker, PSWG Chair
Walter Suarez, PSWG Co-Chair
HITSC Meeting, April 24, 2014

Privacy and Security Workgroup

Health IT Standards Committee
A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

- Dixie Baker - Martin, Blanck, and Associates (Chair)
- Lisa Gallagher – HIMSS (Co-Chair)

- John Blair - Taconic IPA
- Mike Davis – Department of Veterans Affairs
- Leslie Kelly-Hall - Healthwise
- Chad Hirsch - Mayo
- Peter Kaufman - DrFirst
- Ed Larsen
- David McCallie - Cerner Corporation
- John Moehrke - General Electric
- Wes Rishel - Gartner
- Kevin Stine - NIST
- Walter Suarez - Kaiser Permanente
- Sharon Terry - Genetic Alliance

Purpose and Objectives of the Hearing

Purpose: Provide the PSWG with insights into the current status and readiness of the National Strategy for Trusted Identities in Cyberspace (NSTIC) for consideration in determining and recommending standards for the healthcare industry.

Objectives: The objectives of this public hearing were to review and discuss the following topics from a variety of perspectives, including government, standards developers, information security vendors, electronic health record system vendors, and health care providers:

- Current status of NSTIC
- Standards involved in deploying the NSTIC Strategy
- Experiences and findings from NSTIC Pilots
- Healthcare Industry Perspectives on NSTIC

Hearing Agenda, Panels, and Testifiers

Introductions from PSWG Chairs

Overview of NSTIC and Current Status of Development and Implementation

- *Jeremy Grant* - National Institute of Standards and Technology (*NIST) Program Office*
- *Peter Brown and Tom Sullivan - Identity Ecosystem Steering Group (IDESG)*
- *Anil John - Federal Identity, Credential, and Access Management Trust Framework Solutions Program (FICAM), GSA*

Panel 1: NSTIC Ecosystem and Identity Management Standards

- *Eve Maler* - Forrester Research
- *Nat Sakimura* - OpenID Foundation (OIDF)
- *John Bradley* - Ping Identity
- *George Fletcher* - AOL *Inc.*

Panel 2: NSTIC Pilots – Implementation Experiences and Lessons Learned

- *Cathy Tilton* - HealthVault Pilot
- *Michael Farnsworth* - Binary Structures Corporation
- *Douglas Glair* - Federal Cloud Credential Exchange (FCCX) Program - USPS

Panel 3: Healthcare Perspectives on NSTIC and Management Standards

- *Lisa Gallagher* - HIMSS
- *Arien Malec* - CommonWell
- *Kevin Isbell and Tim McKay* - Kaiser Permanente/Care Connectivity Consortium
- *Mike Davis* – Department of Veterans Affairs

Observations: NSTIC Overview Panel

- NSTIC is a national strategic initiative to foster competitive development of stronger identity and identity proofing standards
  - **NOT** a standards-development effort or individual identity program.
  - Need for a range of identity options, from anonymity/pseudonymity to fully identified
  - Different settings or contexts require different identity levels of assurance
- NSTIC is intended to leverage existing credentials across sectors including healthcare
- NSTIC calls for the Federal government to be an early adopter; e.g., Federal Credential Cloud Exchange (FCCX)
- NIST currently collaborating with industry on 12 NSTIC pilots, 6 of which are healthcare-related
- Identity Ecosystem Steering Group (IDESG) is a voluntary public-private partnerships formed to facilitate the development and adoption of a National Identity Ecosystem Framework
  - IDESG's International Coordination Committee helps align NSTIC standards with related international efforts

Observations:
NSTIC Ecosystem and Standards Panel

- Key standards of value to NSTIC implementation:

Technology	NSTIC Value	Comments
OAuth, OpenID Connect, JWT	Immediate high central value	"These provide a backbone of security and portable identity capabilities."
UMA	High central value in the medium term	"UMA uniquely provides capabilities for letting an individual proactively control data- sharing access"
SAML	Moderate central value	"friendlier to large IT shops and web browsers than to smaller organizations and mobile environments — so its reach has limits"
X.509	Moderate and peripheral	"extremely valuable as a security mechanism, [but] as an identity platform … it has struggled"
FIDO	TBD	Authentication specifications that are not (yet) open standards*
XACML	Low peripheral value	

*Open Standards are openly specified and usable protocols, formats, and mechanisms that are free for use (i.e., no access or licensing fees)

Observations:
NSTIC Ecosystem and Standards Panel

- Locating patient data and maintaining an accounting of disclosures are challenges to healthcare
  - UMA profile based on the IDESG Health IT Record Location Service (Data Aggregation) use case may provide usefulness in both areas *(https://www.idecosystem.org/wiki/Health_IT_Record_Location_Service_Data_Aggregation)*
- IDESG will promote and adopt industry standards beneficial to NSTIC
- Majority of large off-the-shelf software providers support OpenID Connect and OAuth 2.0, resulting in very rapid deployments
  - Major companies (e.g., Deutsch Telekom) choose to use OpenID Connect due to its ease and flexibility over SAML, which has never really conformed to the flexibility the social internet requires

NSTIC Pilots Overview

Pilot Name	Use Case	Organizations Involved	Status	Standards
Advancing Commercial Participation in NSTIC Ecosystem	Access to AARP health	NIST, DAON	First phase expected to go live with AARP, June 2014	• SAML • OpenID Connect • Kantara-certified LOA 1-3 non-PKI
Cross-Sector Digital Identity Initiative (CSDII)	Patient and Provider Access to Hospital Portal/EHR	American Assoc. of Motor Vehicle Administrators , Biometric Signature ID, CA Technologies , Commonwealth of VA , Microsoft, Binary Structures.	Preparing for marketplace; Pilot launch in April 2014	• SAML • OpenID Connect • OAuth 2.0 • Can support LOA 1-3 non-PKI
Federal Cloud Credential Exchange (FCCX)	Connects FICAM-enabled multiple government relying parties to a single identity hub	USPS, NIST, GSA	Early stages	• SAML 2.0 • OpenID Connect support on roadmap • FICAM-approved credentials, LOA 1-4

NSTIC Pilots: Lessons Learned

- Pilots demonstrated some of the benefits, value, and challenges relating to interoperable, cross-organization identity credentials
- Trust frameworks that may be widely adopted within the private sector may not be compatible with government-sector frameworks, such as NIST 800-63
- Identity hub that is a convenience for the federal government may constrain innovation and create a single point of failure for the private sector
- Use of EHR demographic data to identity-proof individuals within healthcare may present HIPAA challenges when attempting to use that identity outside of health care
- Some policy questions unique to healthcare
  - Is ability to use a healthcare credential elsewhere desirable and beneficial?
  - Are anonymous/pseudonymous identities useful in healthcare?
  - What is needed to make third-party credentials trustworthy?

NSTIC Pilots: Assessing Readiness for the Healthcare Industry

- Pilots that have moved into production are better candidates for use by the Healthcare industry
- Pilots should involve interoperability across a number of comparable stakeholders
- Pilot report should include some instrument for evaluating the experience of the users and assurance that their needs are being addressed

Healthcare Perspectives (1 of 2)

- Has Launched HIMSS Identity Management Taskforce
  - Multiple stakeholders, including providers and vendors and the NSTIC Healthcare Committee
  - Liaison to national initiatives such as NSTIC
  - Socialize into HIMSS membership and provide tools/resources
  - Focuses on policy and technical challenges relating to identity
- CommonWell Health Alliance
  - Organizational identity is most important for provider-level information exchange
  - Higher-assurance identifiers would be very useful for patient identity matching and linking
  - Recommends higher-assurance identifiers be constructed from third-party credentials (i.e., driver IDs)

Healthcare Perspectives (2 of 2)

- Kaiser Permanente
  - Matching of patients across providers is a patient safety issue
    - Recent study showed identity matching between 40-60%
  - Verified and portable patient identity would enhance matching outcomes on a much broader scale
  - Security provisions should be usability tested by target populations to make sure they do not widen the digital divide
- Department of Veterans Affairs Pilot
  - 3rd-party credential was used to generate an authorized request to VA's authentication federation portal
    - NIST compliant
    - Remote identity proofing
    - Password authentication with security questions and device authentication and verification

Conclusions Gleaned from Hearing

- Hearing helped foster a better understanding of NSTIC as a collaboration between the public and private sectors to achieve the capability for federated identity both within the US and throughout the world
- NSTIC should be viewed not a set of new standards, but as an effort to provide a framework (with common principles) that leverages existing standards that are already in wide use – and in fact are the same standards as are used in the new Blue Button+ standard
- The use of high-assurance patient identities can improve the matching of patient records – thereby enhancing patient safety and the quality of patient care
- Active healthcare industry involvement with the IDESG and NSTIC community is needed to help ensure that healthcare use cases are addressed
- Increased collaboration among government healthcare agencies – FDA, DEA, CMS, ONC, and others – is needed to uniformly implement NSTIC in federal health care activities
- Standards should be evaluated for maturity and adoptability, using HIT Standards Committee evaluation criteria

Written Testimonies presented at the hearing are available on ONC site at:

http://www.healthit.gov/facas/calendar/2014/03/12/privacy-security-workgroup's-nstic-public-hearing