

HIT Standards Committee

Observations from Public Hearing: Trusted Identity of Providers in Cyberspace

Dixie Baker, Chair Privacy and Security Workgroup

July 19, 2012

Context

- On Wednesday, July 11, the chairs of the HIT Policy Committee, Privacy and Security Tiger Team (Deven McGraw) and the HIT Standards Committee, Privacy and Security Workgroup (Dixie Baker) jointly led a hearing on Trusted Identity of Providers in Cyberspace
- Focus
 - Identity proofing
 - Identity authentication
 - Provider remote access and cross-organizational exchanges
 - Interoperability of identity proofing and authentication across organizations
 - Consumer identity to be addressed later

National Coordinator Introductory Remarks

- Since the first hearing the HITPC held on this topic, important policy developments have occurred, stimulating the development of market-based identity solutions
 - *National Strategy for Trusted Identity in Cyberspace (NSTIC)* – released by the White House in April 2011; based on four principles:
 - Privacy-enhancing and voluntary
 - Secure and resilient
 - Interoperable
 - Cost-effective and easy to use
 - Update to NIST Special Publication 800-63, *Electronic Authentication Guideline* (December 2011)
 - Identifies minimum technical requirements for remotely authenticating the identity of users
 - Provides guidance for each of the four levels of authentication

National Coordinator Introductory Remarks (cont.)

- “The status quo is not good enough”
 - Should be aiming to develop policy that allows for high level assurance for trusted identity for providers without stifling innovative technology solutions
- Believes that NIST 800-63-1 Level of Assurance (LOA) 3 is a reasonable standard for identity-proofing and authenticating providers
 - Requires verification of identity (e.g., using a Government-issued identifier) in order to receive a credential
 - Requires multi-factor authentication for remote access

NIST 800-63-1 Level of Assurance (LOA) 3

- LOA 3 requires the use of at least two factors for remote-access authentication
- Identity proofing (assurance of the identity of an individual at time of registration & issuance of authenticator)
 - Verification of identifying materials and information (including government-issued picture ID)
- Authentication (proof that the individual is who she claims to be at time of attempted access)
 - At least two factors, typically a key encrypted under a password (not required to be implemented in hardware)
 - Must resist eavesdroppers
 - May be vulnerable to man-in-the-middle attacks (e.g., phishing and decoy websites), but must not divulge authentication key

Panels and Panelists

- **Panel 1 – Understanding the Value of Trusted Identity for Providers**
 - David Hunt, Physician Steering Group on Trusted Identity, ONC
 - Alan Coltri, Chief Systems Architect, Johns Hopkins University
 - Rick Rubin, Chief Executive Officer, OneHealthPort, Washington HIE
 - Dan Porreca, Executive Director, HEALTHeLINK
- **Panel 2 – Trusted Identity: A Changing Ecosystem**
 - Jeremy Grant, Senior Executive Advisor for Identity Management, NIST
 - Tim Polk, Cryptographic Technology Group, NIST
 - Deborah Gallagher, Office of Government Wide Policy, US General Services Administration

Panels and Panelists (cont.)

- **Panel 3 – Trusted Identity Solutions in the Private Sector**
 - Ash Evans, Director, Corporate Strategy, Verizon
 - William R. Braithwaite, Chief Medical Officer, Anakam Identity Services, Equifax
 - Paul L. Uhrig, Executive Vice President, Chief Administrative and Legal Officer, Chief Privacy Officer, Surescripts
 - Thomas E. Sullivan, Chief Privacy Officer, Chief Strategic Officer, DrFirst
 - Steve Kirsch, Founder and Chief Technology Officer, OneID
 - [Scott Howington, Head of Global Programs, SAFE-BioPharma Association, provided written testimony but was not able to participate in the hearing]

Panels and Panelists (cont.)

- **Panel 4 – Trusted Identity Solutions in the Federal Government**
 - Tony Trenkle, Chief Information Officer, CMS
 - Cynthia Bias, Integrated Electronic Health Record (iEHR) Program Office, VA and DOD
 - [John Bossert, Chief, Diversion Technology Section, DEA, was invited but did not participate]

Key Points and Observations (1 of 4)

- No established or de facto standard exists for either ID-proofing or authenticating providers
 - Current state-of-practice is passwords (LOA 2)
 - 5 of top 6 vectors of attack in 2011 data breaches were tied to passwords (health sector #1 target in 2011)
- Focus of identity assurance in healthcare seems to be shifting from the entity/organization level to the individual level – most of the testimony presented focused on the latter
 - However, neither Exchange nor Direct requires identity assurance at LOA 3
 - No recommendation for LOA 3 was included in recommendations for Stage 2 meaningful use
- NIST 800-63-1 LOA 3 authentication is feasible, and consistent with the direction the industry is heading
 - Mobile technologies have emerged as key platform for LOA 3 two-factor solutions

Key Points and Observations (2 of 4)

- The need for a high level of assured identity extends to every other health care provider (nurses, pharmacists, dentists, therapists, etc), and even to administrative staff
- Important to assure that policies and approaches used for assuring the identity of individuals who access health information within an organization are compatible with the need for a high level of assurance of the identity of providers who access and exchange health information with other providers external to the organization

Key Points and Observations (3 of 4)

- Both government and private industry are embracing the Federal Identity, Credential, and Access Management (FICAM) Trust Framework and NIST SP 800-63-1
 - Secure, interoperable and privacy-enhancing process by which federal agencies and private sector can leverage commercially issued digital identities and credentials
 - Four non-federal organizations have been approved to be Trust Framework Providers (TFPs) – who then assess and accredit commercial identity providers who conform to the USG profiles and abide by the privacy criteria
 - Kantara*
 - InCommon*
 - SAFE Bio-Pharma*
 - Open Identity Exchange (OIX)*
 - CMS has identified risks that warrant LOA 3 assurances and will use FICAM-certified credential providers to meet this need

Key Points and Observations (4 of 4)

- Support and momentum for the NSTIC initiative is building – expect NSTIC to emerge as the common basis for identity management for both the private and public sectors
 - Calls for **Identity Ecosystem** – “an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities”
 - Emphasis on authenticating identity without disclosing private information will be appreciated by both the healthcare industry and by consumers
 - Not clear what will cost – business models still emerging
 - Commercial marketplace is developing solutions based upon NSTIC principles and 800-63-1
 - e.g., DrFirst, OneID, Verizon authentication solutions all meet LOA 3 requirements and are consistent with NSTIC principles

NSTIC Privacy and Civil Liberties Principles

- Increase privacy
 - Minimize sharing of unnecessary information – share only “need to know” attributes
 - Minimum standards for organizations – such as adherence to Fair Information Practice Principles (FIPPs)
- Voluntary and private-sector led
 - Individuals can choose to participate or not
 - Individuals who participate can choose from public or private-sector identity providers
 - No central database is created
- Preserves anonymity
 - Digital anonymity and pseudonymity support free speech and freedom of association

Summary Observations

- Momentum toward highly assured identity is building, as several critical forces are aligning:
 1. Increasing awareness of vulnerabilities and workflow impacts associated with use of passwords
 2. Rapidly dropping cost of digital certificates – from 2-or-3-digit pricing per certificate just 5 years ago to less than \$1 to “free” today – resulting in broader adoption in all sectors
 3. DEA is requiring a high (>LOA 3) for all prescribers of controlled substances
 4. VA is using high (>LOA 3) with all of their internal providers, and looking at how to expand to external providers
 5. CMS plans to move “as early as next year” to requiring ALL of its contracted providers to use high LOA identity proofing and authentication when conducting business with Medicare
- Current HIE state-of-practice still relies on passwords – need for a roadmap for progressing toward LOA 3