Privacy and Security Tiger Team

Trusted Identity of Providers in Cyberspace

Recommendations

August 1, 2012

Tiger Team Members

- **Deven McGraw, Chair**, Center for Democracy & Technology
- **Paul Egerman, Co-Chair**
- **Dixie Baker**, SAIC
- **Dan Callahan,** Social Security Administration
- **Neil Calman**, Institute for Family Health
- **Carol Diamond**, Markle Foundation
- **Judy Faulkner**, EPIC Systems Corp.
- **Leslie Francis**, University of Utah; NCVHS
- **Gayle Harrell**, Consumer Representative/Florida
- **John Houston**, University of Pittsburgh Medical Center
- **Alice Leiter**, National Partnership for Women & Families
- **David McCallie**, Cerner Corp.
- **Wes Rishel**, Gartner
- **Latanya Sweeney**, Carnegie Mellon University
- **Micky Tripathi**, Massachusetts eHealth Collaborative

Previous HIT PC Recommendations

- Digital certificates with “high” degree of assurance issued at an entity level, with each entity credentialing its individual users
  - Assuring a trusted “machine to machine” transfer of protected health information
- Individual-level credentials for accessing information across a network (such as NwHIN) should be issued at a level higher than just user name and password [Level of Assurance (LOA) 2]
  - But not prepared to recommend LOA 3 due to perceived burden
- Focused on exchange among providers to meet meaningful use

Recent Developments

- *National Strategy for Trusted Identity in Cyberspace (NSTIC)* – released by the White House in April 2011; focuses on individual user credentials; 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
- Joint hearing of Tiger Team and Privacy & Security Working Group of the HIT Standards Committee on July 11 to explore further

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
- Must not be vulnerable to man-in-the-middle attacks (e.g., phishing and decoy websites) nor divulge the authentication key

Key Points and Observations

- No established or de facto standard exists for either ID-proofing or authenticating providers
  - Current state-of-practice is passwords (LOA 2)
  - About 5 percent of reported HIPAA breaches were associated with unauthorized use on the network (not directly associated with hacking)
- Focus of identity assurance generally seems to be shifting from the entity/organization level to the individual level – most of the testimony presented focused on the latter
- NIST 800-63-1 LOA 3 authentication is arguably more 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

- 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

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 baseline LOA 3

Scope of the Tiger Team Discussion

- The Tiger Team focused on "trusted identity“ – identity proofing and authentication
  - Did not address trusted access or authorization
  - Focused on providers; patient access to be addressed at a later time
  - Continued to focus on exchange transactions needed to meet Meaningful Use
- "Are you who you claim to be?”, with a sufficient level of assurance based on the intended purpose for the exchange of data

Recommendations to the HIT Policy Committee (1/3)

1. The Tiger Team believes that ONC should move toward individual-user level credentials to meet NIST Level of Assurance (LOA) 3 for riskier exchange transactions, ideally by Meaningful Use Stage 3.

Rationale:

- Low risk activity, such as on-site, intra-organizational access to systems/data should not necessitate additional authentication requirements.
- Riskier exchange transactions, such as remote access to systems/data across a network, should require the increased assurance provided by LOA 3.

Exchange Scenarios

Function	LoA*	Risk/Harm
EHR access via local computer/terminal within a secured area	2	Unauthorized personnel may physically access computer
EHR access via local computer/terminal within a publicly accessible area	2	Unauthorized personnel or public may physically access
On premises (hospital/clinic) wireless access to E H R unsecured network		Data transfer in open, Man-in-middle attack sniffing, Unauthorized personnel or public may remotely access
On premises (hospital/clinic) wireless access to EHR via VPN		Theft, unauthorized access/exposure
EHR access via mobile devices off premise	3	Theft, unauthorized access/exposure
Physician HIE access in multiple practices		Unauthorized access
Electronic Prescribing	3+	Fraudulently obtaining controlled substances

*Recommended baseline LOA based on Tiger Team deliberations

Recommendations to the HIT Policy Committee (2/3)

2. As an interim step, the ONC could require baseline two-factor authentication (per NIST 800-63-1) with existing organization-driven identity proofing (LOA "2.5")
   - Two-factor authentication provides additional assurance
   - Entities not yet required to implement more robust identity proofing per NIST 800-63-1
3. Should extend to all clinical users accessing/exchanging data in the riskier exchange transactions.

Recommendations (3 of 3)

4. ONC's work to implement this recommendation should be informed by NSTIC and aim to establish trust within the health care system, taking into account provider workflow needs and the impact of approaches to trusted identity on health care on health care quality and safety.
    - For example, NSTIC also will focus on the capability to pass along key attributes that can be attached to identity. The capability to pass key attributes – e.g., valid professional license – may be critical to facilitating access to data.
5. ONC should consult with NIST about future iterations of NIST 800-63-1 to identify any unique needs in the healthcare environment that must be specifically addressed.

Backup Slides

800-63 Authentication Requirements

LOA2	LOA3
Single factor	Multi-factor
NIST LOA2 Identity Proofing (or higher)	NIST LOA3 Identity proofing (or higher)
Approved cryptographic techniques required	Approved cryptographic required for all operations
Eaves dropper, on-line guessing prevented	Eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks prevented
LOA3/LOA 4 Multi-factor may be used	Minimum of two factors required; 3 token types may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens. Examples: shared secret, mobile one-time- password (OTP) application, PKI, USB token, credit card password tokens, RFID or blue tooth token

LOA2/LOA3 Identity Proofing Required Information

	Level 2	Level 3
In person	Possession of valid current primary Government Picture ID • applicant's picture, and • either address of record or nationality of record (e.g. driver's license or passport)	Level 2 plus •ID must be verified
Remote	• Possession of a valid Government ID (e.g. a driver's license or passport) number *and* • Financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of *either* number.	Same as Level 2 but confirmation via records of **both** numbers.

LOA2/LOA3 Identity Proofing
Registration Authority (RA) In Person Process

Level 2	**Level 3**
Inspects photo-ID, compare picture to applicant, record ID number, address and DoB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	Essentially same as Level 2 ***plus*** **Verify** via the issuing government agency or through credit bureaus or similar databases. **Confirm** that: name, DoB, address and other personal information in record are consistent with the application**.**

LOA2/LOA3 Identity Proofing
Registration Authority (RA) Remote Process

Level 2	Level 3
• Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records **are on balance consistent** with the application and sufficient to identify a unique individual. • Address confirmation and notification: a) Sends notice to an address of record confirmed in the records check or; b) Issues credentials in a manner that confirms the address of record supplied by the applicant; or c) Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or **e-mail at number or e-mail address associated with the applicant in records.**	• Verifies information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records **are consistent** with the application and sufficient to identify a unique individual. • Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, **while recording the applicant's voice.**

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]

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

Additional Key Points and Observations

- 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