National Strategy for Trusted Identities in Cyberspace

ISPAB Briefing

Mike Garcia

National Institute of Standards and Technology (NIST)

June 12, 2015

Why NSTIC?

1. Kill the password dead
   - "Perfect combination of awful security and awful usability"

2. Help address the "Dog on the Internet problem"
   - Key to enabling high-value online transactions (both in government and private sector, i.e., electronic health records) is solving the "identity conundrum" – are you really who you say you are?

3. Improve privacy
   - Give individuals more control over what attributes are disclosed and how they are used (and reused).

Cybersecurity, cloud, big data, privacy – it's hard to get any of them right without solving identity.

The solution: an Identity Ecosystem

NSTIC calls for an **Identity Ecosystem**, "an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards (both technical and policy) to obtain and authenticate their digital identities."

Guiding Principles

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

How is NSTIC different?

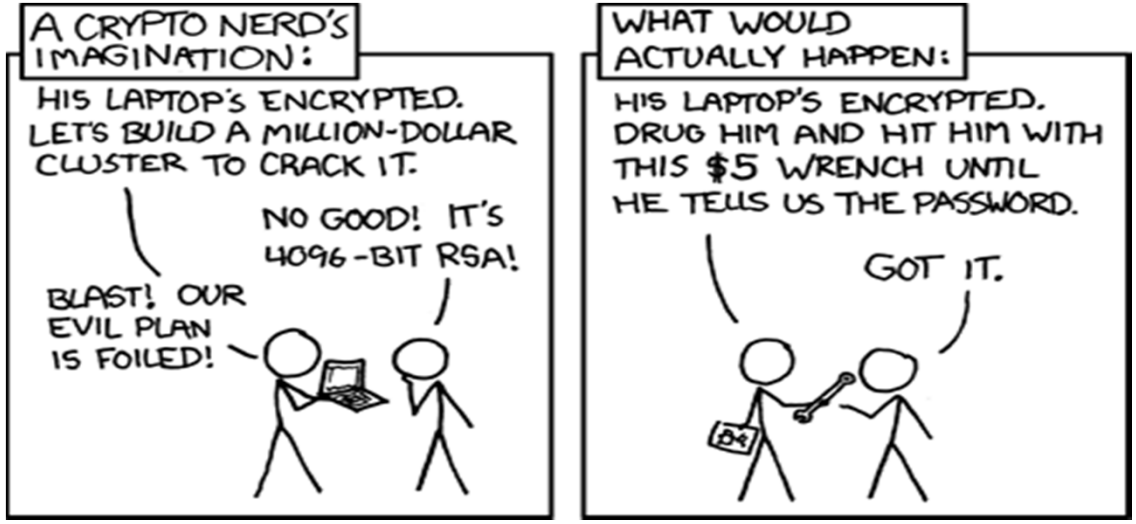
The NSTIC approach is about a marketplace for solutions

- **When solutions break, they can go away**
- **When new solutions emerge, they can make inroads.**

There is a marketplace today – but there are barriers the market has not yet addressed on its own.

Government can serve as a convener and facilitator, and a catalyst.

Barriers: It's not all about security



Source: *xkcd*

Usability

Liability

Privacy

Business Models

Interoperability

Key Implementation Steps

Convene the Private Sector

- August 2012: Launched privately-led **Identity Ecosystem Steering Group (IDESG).** Funded by NIST grant, IDESG tasked with crafting standards and policies for the Identity Ecosystem Framework http://www.idecosystem.org/
- October 2013: IDESG incorporates as 501(c)3, prepares to raise private funds
- Leadership includes Citi, Lexis-Nexis, Symantec, Oracle, Aetna, US Bank and Neiman Marcus – as well as AARP, Patient Privacy Rights, and other advocates.

Fund Innovative Pilots to Advance the Ecosystem

- 4 rounds of pilot grants since 2012, 5th round expected to be awarded in September
- 15 pilots funded in total; 11 now active

Government as an early adopter to stimulate demand

- White House effort to create **Connect.gov**, a single service for identity at public facing government applications.
- October 2015: Executive Order 13681, requiring all USG digital applications that release personal data to require Multi Factor Authentication (MFA) + an effective identity proofing process

Where do we stand?

Pilots have moved the marketplace

$30M awarded to 15 pilots over three years

- Brought together a community of more than 125 firms and organizations to partner with each other in support of advancing the NSTIC
- Impacted more than 2.3 million Americans, who are now using NSTIC-aligned credentials across health, education, financial services, government, online retail, and telecommunications sectors.
- Helped 9 new, NSTIC-aligned multi-factor authentication (MFA) solutions reach the market; some of these are being used in the new Connect.gov offering
- Created 4 new Trust Frameworks to enable interoperability of NSTIC-aligned credentials across sectors

Some more on pilot impact…

More than **140 universities** are deploying **smartphone-based MFA** (Internet2)

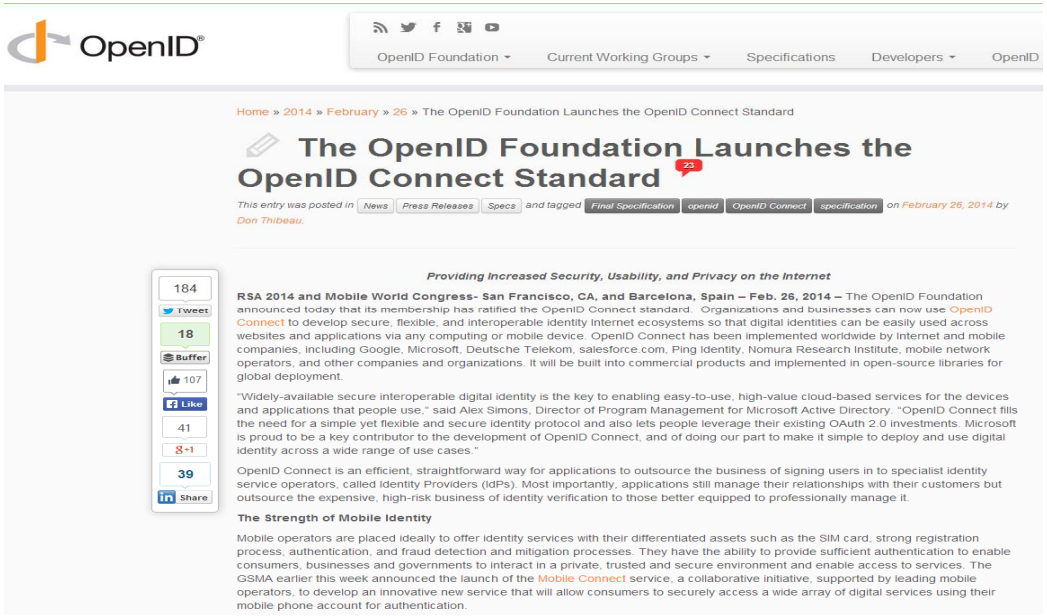
More than **250,000 kids and parents** – **in compliance with COPPA** – are able to access content at websites (PRIVO)

Inova Health Systems will enable **1500 patients** to securely obtain their personal health record, leveraging validated attributes from **Virginia's DMV** (AAMVA)

A Broadridge/Pitney Bowes JV has launched targeting **140 million customers** for **secure digital delivery** of financial services content, bill presentment and bill pay (ID/Dataweb)

More than **1,000,000 Veterans, Teachers and First Responders** can access online services from more than **200 organizations** without having to share documents containing sensitive PII to prove their affiliation (ID.me)

The marketplace has started to respond



OpenID®

OpenID Foundation ▾ Current Working Groups ▾ Specifications Developers ▾ OpenID

Home » 2014 » February » 26 » The OpenID Foundation Launches the OpenID Connect Standard

The OpenID Foundation Launches the OpenID Connect Standard

This entry was posted in News | Press Releases | Specs *and tagged* Final Specification | openid | OpenID Connect | specification *on February 26, 2014 by Don Thibeau.*

184 Tweet 18 Buffer 107 Like 41 +1 39 Share

Providing Increased Security, Usability, and Privacy on the Internet

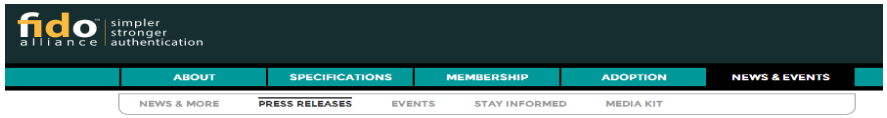
RSA 2014 and Mobile World Congress- San Francisco, CA, and Barcelona, Spain – Feb. 26, 2014 – The OpenID Foundation announced today that its membership has ratified the OpenID Connect standard. Organizations and businesses can now use OpenID Connect to develop secure, flexible, and interoperable identity Internet ecosystems so that digital identities can be easily used across websites and applications via any computing or mobile device. OpenID Connect has been implemented worldwide by Internet and mobile companies, including Google, Microsoft, Deutsche Telekom, salesforce.com, Ping Identity, Nomura Research Institute, mobile network operators, and other companies and organizations. It will be built into commercial products and implemented in open-source libraries for global deployment.

"Widely-available secure interoperable digital identity is the key to enabling easy-to-use, high-value cloud-based services for the devices and applications that people use," said Alex Simons, Director of Program Management for Microsoft Active Directory. "OpenID Connect fills the need for a simple yet flexible and secure identity protocol and also lets people leverage their existing OAuth 2.0 investments. Microsoft is proud to be a key contributor to the development of OpenID Connect, and of doing our part to make it simple to deploy and use digital identity across a wide range of use cases."

OpenID Connect is an efficient, straightforward way for applications to outsource the business of signing users in to specialist identity service operators, called Identity Providers (IdPs). Most importantly, applications still manage their relationships with their customers but outsource the expensive, high-risk business of identity verification to those better equipped to professionally manage it.

The Strength of Mobile Identity

Mobile operators are placed ideally to offer identity services with their differentiated assets such as the SIM card, strong registration process, authentication, and fraud detection and mitigation processes. They have the ability to provide sufficient authentication to enable consumers, businesses and governments to interact in a private, trusted and secure environment and enable access to services. The GSMA earlier this week announced the launch of the Mobile Connect service, a collaborative initiative, supported by leading mobile operators, to develop an innovative new service that will allow consumers to securely access a wide array of digital services using their mobile phone account for authentication.



fido alliance simpler stronger authentication

ABOUT | SPECIFICATIONS | MEMBERSHIP | ADOPTION | NEWS & EVENTS

NEWS & MORE | PRESS RELEASES | EVENTS | STAY INFORMED | MEDIA KIT

FIDO Alliance Opens Technology for First Public Review to an Industry Desperate for Simpler, Stronger Authentication

Mountain View, CA - February 11, 2014 - The FIDO (Fast IDentity Online) Alliance (http://www.fidoalliance.org/), an open industry consortium delivering standards for simpler, stronger authentication, achieved a historic milestone today by releasing its first public review draft technology specifications. These open technologies have been collaboratively developed by a rapidly increasing number of the most innovative companies in the world to enable simpler, stronger authentication to scale in the market.

The Q1 2013 Forrester Wave™: Enterprise Fraud Management asserts the online services industry is seeing upwards of $200B in annual losses from password breaches and related hacks that exploit the vulnerabilities inherent in single-factor password systems. According to the Verizon 2013 Network Investigations Data Breach Report, 76 percent of network intrusions exploit weak or stolen credentials. According to Gartner, 20 to 50 percent of all help desk calls are for password resets. Forrester Research estimates help desk labor cost at $70 per password reset*. In Mobile Consumer Insights, Jumio reports that 68 percent of smartphone and tablet owners have attempted to make purchases on their device. Due to problems during

Making it all work together

- **Critical rule: Don't turn 40 passwords into 40 smartcards, OTP tokens, apps, etc.**
- **We can avoid this with a framework of standards and operating rules that enables interoperability**
- **Both at a technical and policy level**

The Identity Ecosystem Steering Group (IDESG)

- 350+ members, including: US Bank, Verizon, Visa, PayPal, Fidelity, Citigroup, Mass Mutual, IBM, Bank of America, Microsoft, Oracle, 3M, CA, Symantec, LexisNexis, Experian, Neiman Marcus, NBC Universal, Aetna, Intel
- Also: AARP, ACLU, EPIC, EFF, and more than 65 universities. Participants from 12 countries
- NIST awarded new 3-year grant to IDESG, Inc., last July
  - Old grant: pay for firm to convene IDESG, provide administrative support
  - New grant: augment admin support with technical resources to accelerate framework deliverables
- Hired as first full-time executive director
- V.1 of Identity Ecosystem Framework due this summer.

What's the Identity Ecosystem Framework?

- For version 1: A set of business rules and requirements and a set of adopted interoperability standards to which organizations self-attest
- In the future: v1 + accountability mechanisms, risk models, liability arrangements, and trustmark scheme or method of digital verification
- When participants wish to interact with other participants, they know that they are interoperable beyond the technical level
- When specialized requirements are necessary for a community of interest, those requirements can be build on top of the IDEF's baseline

NSTIC: What Comes Next?

Keep doing the good stuff, increase focus on the science and tech

- Continue to run a pilots program, but evolve towards a focus on specific use cases and gaps that emerge in the market
- Be more NISTy: address foundation barriers the market faces
  - Performance standards for biometrics
  - Deployable privacy enhancing technologies
  - More work like the IRS study
  - 800-63 update
  - Strength of credential, strength of proofing, comparability
- Make Connect.gov a breeze: more from Paul

NSTIC: Priority Activities

Short and medium terms

Fulfill critical needs

- 800-63: review comments, establish update plan
- Connect.Gov strategy
  - shared services for MFA, proofing
  - attribute encryption
  - identity resolution methodology
- Market research and analysis
- Pilot support, program targeting
- IDESG financial and staff support

Long term

Address evolving market impediments

- Transition of pilots program
- Increase technical capacity
  - standards development
  - reference materials
  - open source development
  - test beds
  - toolkits
- IDESG support as member

Thanks!

Michael Garcia
NSTIC National Program Office
National Institute of Standards and Technology
michael.garcia@nist.gov
www.nstic.gov
@NSTICNPO

16