PDEC: The Personal Data Ecosystem Consortium

www.pde.cc @personaldata

PDEC Report 2013-01

What could kill NSTIC?

A Friendly Threat Assessment In Three Parts

January 2013

by Phil Wolff, Strategy Director, PDEC. phil@pde.cc. @evanwolf.

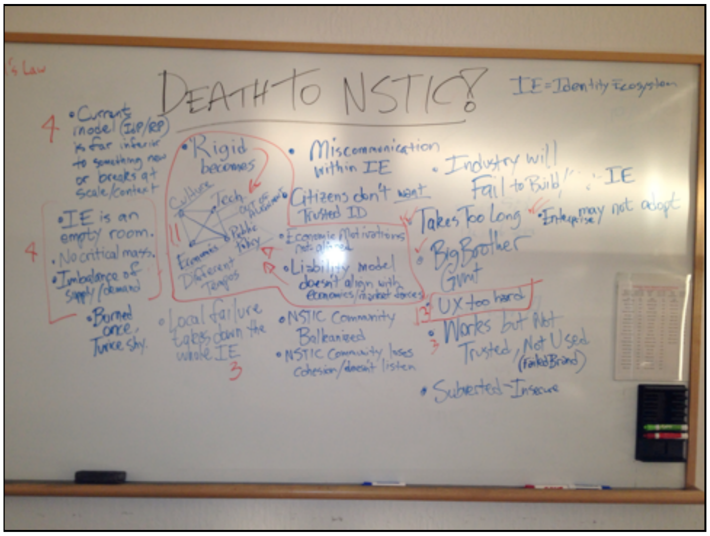
Phil Wolff is a technologist and industry analyst, with a public policy streak. He was a director of the DataPortability Project and is a technology leadership alum of Adecco SA, Bechtel National, Compaq Computer, LSI Logic, US Navy Supply Systems Command, and Wang Labs.

In short: The two most serious threats: a user experience that doesn't work and imbalance among the forces that hold an identity ecosystem together.

High hopes fly for an international identity system that works across industries, technologies, governments, regulatory schemes and still manages to be user centric. This is driven in the United States under a program initiated by the National Strategy for Trusted Identity in Cyberspace through the National Institute of Standards and Technology (NIST).

A dozen of us met at Internet Identity Workshop 15 in October 2012 to list and score threats to the NSTIC Identity Ecosystem vision. We did the same thing in May 2011. We asked: **if NSTIC fails by 2016, what could have brought it down?** Here's our hypothetical CY 2016 post-mortem.

1. FROM THE COMPUTER HISTORY MUSEUM IN MOUNTAIN VIEW, CALIFORNIA...


DEATH TO NSTIC?
IE = Identity Ecosystem
4
• Current model (IdP/RP) is far inferior to something new or breaks at scale/context
• Rigid becomes
Culture
Tech
Out of alignment
Public Policy
Economics
Different Tempos
11
• Miscommunication within IE
• Citizens don't want Trusted ID
• Economic Motivations not aligned
• Liability model doesn't align with economies/market forces
• Industry will Fail to Build IE
• Enterprise may not adopt
Takes Too Long
• Big Brother Gvmt
UX too hard
12
• Works but Not Trusted, Not Used (Failed Brand)
3
• Subverted - Insecure
4
• IE is an empty room.
• No critical mass.
• Imbalance of supply/demand
• Burned once, Twice shy.
• Local failure takes down the whole IE
3
• NSTIC Community Balkanized
• NSTIC Community loses cohesion/doesn't listen

We didn't cooperate to build an ID ecosystem. We should have played well with others.

- Took too long. Strung out by process problems.
  (Alternatives emerged.)

- Industry failed to build it.
  (Capital and management didn't prioritize.)

- NSTIC community became balkanized. NSTIC community lost cohesion; didn't listen to each other.
  (Little to no interop.)

- The program was co-opted by a Big Brother government.
  (Not trustworthy internationally and for many purposes.)

Just because it's built doesn't mean they'll use it.

- Worked, but was not trusted.
  (Failed Brand).

- Was subverted and insecure.
  (Legitimately Untrusted).

- Enterprise didn't adopt it.
  (Business case not well made.)

- After one failure, supporters abandoned the project. "Burned once, twice shy."
  (Shallow, brittle commitment; low tolerance for failure.)

- The IE was an empty room. No critical mass formed. There was an imbalance of supply and demand.
  (Anchor tenants didn't sign on. Institutions didn't enroll millions of users or pull in industry ecosystems.)

- Citizens didn't *want* trusted identity.
  (Poor market fit; lack of perceived benefit over alternatives.)

We didn't build the right things the right way.

- A local failure took down the whole identity ecosystem.
  (Failures of ecosystem trust, architecture, integration testing, and risk analysis.)

- The IdP/RP/Trust identity model was inferior to newer models.
  (Technology risk.)

- The IdP/RP/Trust identity model broke at scale or broke in diverse contexts.
  (Project design risk.)

- Miscommunication within the Identity Ecosystem contributed to its death. (Poor cooperation, weak community, high self interest, low trust.)

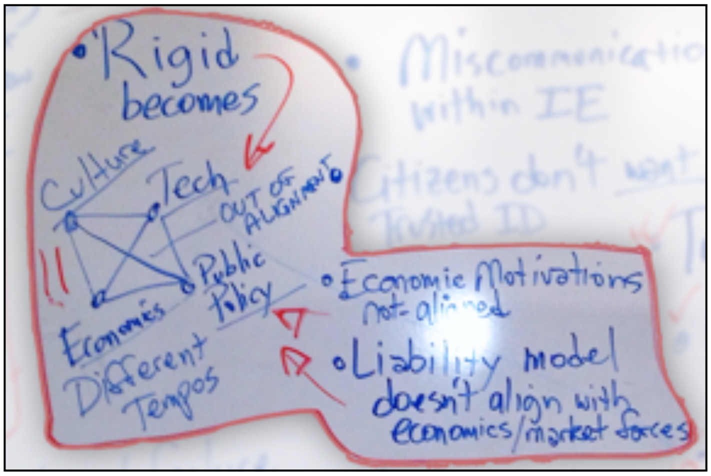
Failed User Experience.

- UX was too hard.
- Everything went wrong that could go wrong.

We Built-In Structural Instability.

Along with user experience, structural instability was the big issue, according to the group…

Technology, economics, policy and culture must be strong. Each relationship among them was imbalanced.


Rigid becomes
Culture
Tech
OUT OF ALIGNMENT
Public Policy
Economics
!!
Different Tempos
Economic Motivations not aligned
Liability model doesn't align with economics/market forces
Miscommunication within IE
Citizens don't want Trusted ID

Each of these pillars were operating on different **tempos**. It was fast to iterate improved user experiences but slow to socialize each round among public policy and enterprise lawyers, for example.

Motivations were misaligned. Some companies, for example, engineered tariffs for data sharing into their terms of service, cutting off public sector and NPOs from their customers.

Core ideas didn't survive translation. Several large Internet engineering companies backed out of supporting IE infrastructure because the "Easy ID" brand became a running joke on sitcoms, SNL, and a biting meme on YouTube.

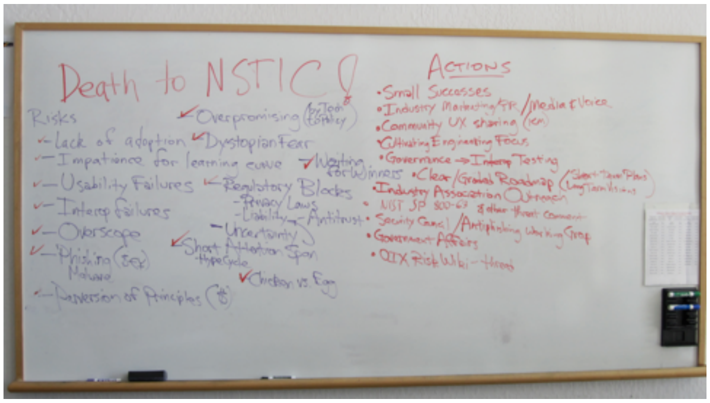
Liability was broken. Tragic risks were taken with some technologies and contracts by pushing exposure from those who enabled risk to those who didn't.

This session was in October 2012.

But wait, there's more…

2. EIGHTEEN MONTHS EARLIER…

We did a similar exercise 18 months earlier in May 2011 with a similar group.


Death to NSTIC!
Risks
-Lack of adoption
-Impatience for learning curve
-Usability Failures
-Interop failures
-Overscope
-Phishing (SEX) Malware
-Perversion of Principles
Overpromising (by Tom Smedinghoff)
Dystopian Fear
Waiting for Winners
Regulatory Blocks
-Privacy Laws
-Liability
-Antitrust
-Uncertainty
Short Attention Span
-Hype Cycle
Chicken vs. Egg
Actions
•Small Successes
•Industry Marketing/PR/Media & Voice
•Community UX sharing
Cultivating Engineering Focus
•Governance → Interop Testing
•Clear/Global Roadmap (Short-Term Plans / Long-Term Visions)
•Industry Association Outreach
•NIST SP 800-63 & other threat comment
•Security Council/Antiphishing Working Group
•Government Affairs
•OIX Risk Wiki - threats

https://secure.flickr.com/photos/philwolff/5713880402/ cc-by Phil Wolff

Key Risks:

- Lack of adoption.
- Impatience for long learning curve.

- Usability failures.
- Interop failures.
- Overscope.
- Security problems like phishing and malware drawn by money.
- Perversion of principles.
- Chicken vs. Egg problems.
- Short Attention Span and the Hype Cycle
- Regulatory blocks including privacy laws, antitrust concerns and uncertainty about liability
- Waiting for Winners
- Dystopian Fear
- Over-promising by tech to policy communities

We had time, in this session, to brainstorm what might avoid or mitigate these threats.

Actions:

- Small successes
- Industry marketing, PR, Media/Voice
- Community user experience sharing (KM)
- Cultivating Engineering Focus
- Governance driving Interop Testing
- Clear/Graded Roadmap (short term plans with long term visions)
- NIST SP 800-63 and other threat comment
- Security Council / Antiphishing Working Group
- Government Affairs activity
- OIX Risk Wiki

What changed between the two session?

The fear of "failure to deliver" was still there.

Outside forces like dystopian fear among users, security failures, and regulatory challenges were less prominent or not mentioned. But the drivers of failure expanded almost exclusively to internal ones.

The primary concern: now that funding, staffing, and collaboration have started: the identity ecosystem will not take charge and master the challenges as they emerge.

3. LAST MINUTE UPDATE...

COASTWISE 1
VICTORIA PARK
Arbroath – Auchmithie
Climber air-lifted after cliff accident
Someone in Trouble? DIAL 999 Ask for the COASTGUARD
SCHOOLGIRL HAD 'NO CHANCE OF ESCAPE'
STAY ON THE CLIFF PATHS

. Arbroath Cliffs Warning Notice CC-BY-NC Alan Parkinson

Cuts are coming to US federal government spending in the new year as we prepare this paper in December 2012. Cuts will come by cleaver if a "fiscal cliff avoiding" budget is passed or with a chainsaw if Congress and the President fall over the "cliff."

Direct effects. Nobody knows if this will directly affect NIST and the NIST staff managing the NSTIC project. Could the stream of funding for NSTIC innovation grants dry up and will existing projects be halted? Will NIST's funding for the Identity Ecosystem's Secretariat, that coordinates and supports the work of the IE, be sustained or cut? In a trillion dollar budget, today's spending on NSTIC is a rounding error.

Indirect effects. We don't know how cuts in federal spending will affect the program indirectly as participating organizations lose government contracts, experience greater risk, or enjoy new opportunities.

eGovernment as customer. We also don't know if the largest government agencies that would be among the first implementers of these open, user-centric, trust networks will stay in the game. Having huge customers as "anchor tenants" provides strong incentives for the private sector to invest and make the identity ecosystem work. Will spending cuts interfere with project continuity? Will key personnel stay engaged?

Lots of unknowns.

And no strategy to respond to these risks from the Identity Ecosystem Steering Group. Yet.

Further Reading and Resources

https://pensivepeter.wordpress.com/2012/10/23/death-to-nstic-long-live-nstic/

https://skydrive.live.com/?cid=9a70d9142ec4cc44&id=9A70D9142EC4CC44!827&sff=1

BONUS!

Four NSTIC Questions for Kaliya.

By Kaliya Hamlin

Kaliya Hamlin, PDEC's founder and executive director, *has been involved with NSTIC since before the first draft was published. She attended in person all but one of the NSTIC convened public events since it was announced at an event at Stanford University in March of 2010. She presented about PDEC at the NSTIC Privacy workshop in June 2011, at a panel on a special session within RSA in February 2012 and most recently at the Smart Card Alliance in December 2012. She responded to the NSTIC NPO's Notice of Inquiry asking how to govern the Identity Ecosystem (you can read it here) at their request. She ran for and won a seat on the Management Council as the Citizen and Consumer Advocate Delegate, representing Planetwork with her professional persona as "Identity*

Woman," Saving the World with User Centric Identity & Personal Data.

Q1. What triggered the whole NSTIC thing?

When the Obama administration came into office in 2008, it started a cyber security review. Password re-use was identified as a real threat. Simply put, the fact that people use the same password for multiple sites where they also use the same user-name, likely their e-mail address, is a vulnerability. People use the same password at a small unimportant site with low security where, if compromised, the same user-name/password combination would work to access their accounts on more important and secure sites. This is a vector for privacy, identity theft, and national security.

One result of the cyber security review was the development of a National Strategy for Trusted Identities in Cyberspace (NSTIC).

Another thread that lead to NSTIC was the ongoing work of the Federal Identity and Access Management (FICAM) sub-committee of the Chief Information Officer Council within the General Services Administration. They were working on the challenges of how to support citizens logging into government sites (Departments of Health, Education, Social Security Administration, etc.) to access services government services. These agencies often don't need to know who a citizen is when offering them services, like looking up things in a government library. When it comes to sharing records with a citizen, like tax or educational loans or anything very personal, the government must assure the citizen is who they say they are. NSTIC is supporting a larger conversation about how to enable government trusting private sector issued credentials used by citizens to login to government sites to access services.

Q2. What does the NSTIC program look like now?

There are six parts.

NSTIC National Program Office. The NSITIC NPO operates within the Department of Commerce's National Institute of Standards. It is lead by Jeremy Grant. The office has several full time staff and they are responsible for the transition of NSTIC from a US government initiative to an independent, public-private organization. They're smart, talented, and they care.

NSTIC NPO

@NSTICNPO

The official handle of the National Program Office of the National Strategy for Trusted Identities in Cyberspace

Washington, D.C. · http://www.nist.gov/nstic/

Identity Ecosystem Steering Group (IDESG). The NPO invited many people, NGOs, government bodies, and companies to participate in building an identity ecosystem in the Identity Ecosystem Steering Group. All the people and organizations who sign up to be a part of this are together called "The Plenary." The NSTIC NPO wrote IDESG's charter and its first bylaws.

Identity Ecosystem Steering Group

National Strategy for Trusted Identities in Cyberspace (NSTIC)
NSTIC Secretariat

Home / About / Steering Group Structure / Secretariat

Secretariat

Trusted Federal Systems, Inc.

Trusted Federal Systems, Inc. (TFS) is a systems integrator serving the federal government. Our experienced staff provides solutions which empower agencies to achieve a higher level of performance. We manage, architect, design and implement collaboration and information sharing solutions for government agencies resulting in improved organizational effectiveness. On Thursday July 12, 2012 TFS received notice of a grant award from the National Institute of Standards and Technology to serve as the formal convener and secretariat for the soon-to-be-established Identity Ecosystem Steering Group. As a systems integrator for the federal government, TFS has extensive, hands-on experience in implementing solutions where the authentication of a user's identity is a prerequisite in support of national interests. As a recognized specialist in federated identity management solutions, TFS designed and architected U.S. Department of Justice (DOJ)'s "Trusted Broker Model" which was later implemented as a pilot by Covisint. This architecture is also the basis for FBI's recent roll out of an upgrade to LEO (Law Enforcement On-line). However, as the Secretariat the TFS role is "not to participate" in the Steering Group as a stakeholder, but "to support" the Steering Group by leveraging the strength of our team's experience in process and facilitation methodologies.

Federated Login

To login to the site, click one of the providers above. If you don't want to use Google or Yahoo to login, click Janrain to create an OpenID. More information.

Powered by PingFederate

Site Search

Search

Policies

- Rules of Association
- Membership Agreement
- IPR Policy
- "DRAFT" Committee Charters

IDESG Management Council. The IDESG management council is elected by the members of the plenary who self-selected into stakeholder categories. Each stakeholder category elects a delegate to the Management Council. The entire plenary also elects two at-large positions and two leadership positions. The management council creates sub-committees to get its work done. I'm chairing one that collects holistic ecosystem pictures, for example.

Committees within the IDESG Plenary. These committees do the actual work of making the identity ecosystem's vision a reality. New committees can be proposed by any member. Committee membership is open to all plenary members. The work and activity of the committees is shared openly. A few of the active committees are working on standards, privacy, trust frameworks, accreditation, and nymrights.

The Secretariat. The NSTIC NPO awarded a $2.5 million dollar contract to provide support services to the Identity Ecosystem Steering Group. Trusted Federal Systems won the contract to act as the IESG's "Secretariat." They coordinate meetings, manage listservs, and the like.

NSTIC Pilot Projects. In early 2011, the National Program Office put forward $10 million in funding for five pilot projects that worked to solve some of NSTIC's challenges. Grants were awarded in September 2012 and run for one year. The pilot projects were set up before the IDESG existed and the IDESG had no input into the selection of the the winning pilots. 187 different initial pilot projects applied for grants, 27 were selected to submit full proposals, and five were selected. Applications for a second round of pilots are coming in Q1 2013.

Right now, there's a lot of activity. Many of the groups have weekly conference calls and are working to define their goals, name their concerns, and agree on achievable road map milestones. Most of the administrivia basics are done.

Q3. Lawyers like the term "trust framework." Is there a better framing?

I prefer "accountability framework." Here's why.

Trust is a meta-goal for the overall system and transactions within it. I think naming the techno-legal policy sandwiches "trust frameworks" is a mistake.

These frameworks, which are the Identity Ecosystem's default, connect the Identity Ecosystem's participants through technology, contractual, and economic layers. Each of these layers have their own design and implementation challenges. Making the layers support each other is another kind of challenge. We expect accountability framework layers to complement each other, reinforcing constructive behavior, leading to a healthy ecosystem.

Credit card networks work this way. They connect banks, merchants, and individuals to each other in ways that build trust in the network, pay for the network, and manage individual and network risks.

Legal liability and political concerns are thorny. If a citizen uses a bank-issued digital identity credential to login to the IRS, who is liable if something goes wrong? These "trust frameworks" combine technology interop and contractual policy frameworks that help the parties "trust" identities (believe they are accurate) issued by another party in the system. Within a section of my NSTIC NOI response, I suggested a better name for the frameworks might be "accountability frameworks." http://www.identitywoman.net/the-trouble-with-trust-the-case-for-accountability-frameworks

The issue at its core is about how "trust" means different things in different contexts at different scales. Regular citizens participating in a "trust framework" will think all the people and entities within a "trust framework" are trustworthy and the underlying policies are good and respect people's data and identities. That's not necessarily true. All a trust framework's rules do is name the policies for a particular system; these may not be good for users or organizations within them.

The path to bringing a thriving personal data ecosystem into being will be through the development of multi-party networks using rules (accountability frameworks) in alignment with people, and that respect the individual. Let's look for inspiration to the ways the banking/credit card network exchange valuable information/ currency. You can see designs that manage risk and liability, and create accountability with trust-frameworks/system rules for digital systems.

Q4. Why does PDEC care about NSTIC?

I am focused on making a *personal data* ecosystem (PDE) real. And a rich, strong, diverse *identity* ecosystem lowers common barriers PDE participants confront.

The big vision of an Identity Ecosystem articulated in NSTIC goes well beyond identity credentials for verified identities. It envisions a future with both the technical and policy infrastructure needed for people to share all types of personal data associated with themselves.

NSTIC efforts in these areas will help a personal data ecosystem emerge more quickly :

- Stronger logins. Multi-factor authentication is helpful/useful for a personal data ecosystem to help people protect their personal clouds / personal data stores.
- Work with "real" names. People have records in services that use their "real names" like utility companies, health records, phone companies, governments, businesses. They must "prove" who they are before these risk averse services permit copying their data into their personal data banks.
- Support anonymity. Let people use pseudonyms in transactions.

NSTIC is a *Regulate Forward* strategy

The US government is keen for markets to solve Internet information sharing, privacy and trust challenges. Theirs is a "Regulate Forward" approach. NSTIC strives to establish policy for where technology will be instead of regulating for where it's been: past societal conditions, rapidly obsolescing technologies, and old industry models.
"A good hockey player plays where the puck is. A great hockey player plays where the puck is going to be." — Wayne Gretzky

Aftermatter

PDEC Education

Are you ready to get your team designing your enterprise's personal data strategy?
PDEC offers on-site seminars in 2013 Q1.

Our "Personal Data Economy" on-sites come in three flavors. We have a one day seminar, a deep dive. We have a version of the seminar you can customize, with follow-up conference calls, and a second instructor. And we offer a two-day workshop for project initiation, with the first day a seminar and the second day applying what you've learned to constructing your short term plans and small data roadmap. Read about it or chat with Phil Wolff, phil@pde.cc or +1.510.444.8234.

http://pde.cc/education

PDEC Directory

People and organizations you might want to talk to.
All information is public.
Send additions and corrections to newsroom@pde.cc.

Azigo. CEO: Paul Trevithic. @azigo. http://azigo.com/

Allfiled. CEO: Piyush Shah. @allfiled. http://www.allfiled.com/

bitWorld. Executive Director: Cameron Hunt. http://www.bitworld.us/

Cloudstore. CEO: Johannes Ernst. @cldstr. http://cldstr.com/

Comradity. CEO: Katherine Worman Kern. @comradity. http://www.comradity.net

Connect.me. Co-Founder: Drummond Reed. @respectconnect. http://www.connect.me

Consumer Data Rights. CEO: Craig Lipman. http://consumermarketingrights.org/

Gluu. CEO: Mike Schwartz. @gluufederation. http://www.gluu.org

Interest Networks. CEO: Barbara Bowen. http://www.interestnetworks.com/

Knowledge Based Opportunities CIC. CEO: John Beer. http://kbocic.co.uk/

Kynetx. CEO: Sephen Fuller. @kynetx. http://www.kynetx.com

LifeDash. President and CEO: Travis Bond. @lifedash. http://www.lifedash.com/

MetaConnectors. Project Leader: Victor Grey. http://metaconnectors.com/

MMINDD Labs. CEO: Estee Solemon Gray. @estee http://mmindd.com

My Info Safe. CEO: Ross Hoghson. @myinfosafe. http://www.myinfosafedirect.com/

Mydex. CEO: David Alexander. @mydexCIC. http://mydex.org/

MyMindshare. CEO: Jim Bursch. http://mymindshare.com

OwnYourInfo. Functional Lead: William McCusker. http://ownyourinfo.com

PeerCraft. CEO: Henrick . @peercraft. http://www.peercraft.com/

Personal. CEO: Shane Green. @personal. http://www.personal.com

Personal Info Cloud. Principal: Thomas Vander Wal. @infocloud. http://personalinfocloud.com/

PiB. CEO: John Harrison. http://www.pib-d.net/

Planetwork. Executive Director: Jim Fournier. @planetworkngo. http://www.planetwork.net/

Privo. CEO: Denise Tayloe. http://www.privo.com

Privowny. CEO: Herve Le Jouan. @privowny. http://www.privowny.com/

Project Danube. Project Leader: Markus Sabadello. @privowny. http://www.projectdanube.org

Qiy. CEO: Maarten Louman. @qiytweet. http://www.qiycorporate.nl/en/

Reputation. COO: Owen Tripp. @Reputation_Com . http://www.reputation.com

Reputation. Senior Director, Business Director: Noah Lang. @Reputation_Com . http://www.reputation.com

Reputation. CEO: Michael Fertik . @Reputation_Com . http://www.reputation.com

Singly. CEO: Jason Cavnar. @singlyinc. http://www.singly.com

Switchbook. CEO: Joe Andrieu. @switchbook. http://www.switchbook.com

Synergetics. CEO: Luk Vervenne. http://synergetics.be/

Tangled Web. CEO: Ankit Kapasi. @tangledp2p. http://www.tangledp2p.com

The Customers Voice. CEO: Iain Henderson. @tcvuk. http://www.thecustomersvoice.com/

Virtrue. CEO: Adam Spector. @virtrue. http://www.virtrue.us/