# Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

## Archived Publication

| | |
|---|---|
| **Series/Number:** | NIST Internal Report (NISTIR) 8054 |
| **Title:** | NSTIC Pilots: Catalyzing the Identity Ecosystem |
| **Publication Date(s):** | April 2015 |
| **Withdrawal Date:** | March 15, 2016 |
| **Withdrawal Note:** | NISTIR 8054 is superseded in its entirety by an errata version that includes updates as of 9/20/2015. |

## Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

| | |
|---|---|
| **Series/Number:** | NIST Internal Report (NISTIR) 8054 |
| **Title:** | NSTIC Pilots: Catalyzing the Identity Ecosystem |
| **Author(s):** | K. Megas; P. Lam; E. Nadeau; C. Soutar |
| **Publication Date(s):** | April 2015 (including updates as of 9/20/2015) |
| **URL/DOI:** | http://dx.doi.org/10.6028/NIST.IR.8054 |

## Additional Information (if applicable)

| | |
|---|---|
| **Contact:** | Applied Cybersecurity Division (Information Technology Laboratory) |
| **Latest revision of the attached publication:** | NISTIR 8054 (as of March 15, 2016) |
| **Related information:** | http://www.nist.gov/nstic/ |
| **Withdrawal announcement (link):** | N/A |

National Institute of Standards and Technology
U.S. Department of Commerce

Date updated: March 15, 2016

NISTIR 8054

# NSTIC Pilots: Catalyzing the Identity Ecosystem

Katerina Megas
Phil Lam
Ellen Nadeau
Colin Soutar

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8054

National Institute of Standards and Technology
U.S. Department of Commerce

**NISTIR 8054**

# NSTIC Pilots: Catalyzing the Identity Ecosystem

Katerina Megas
Phil Lam
Ellen Nadeau
*NSTIC National Program Office*
*Information Technology Laboratory*

Colin Soutar
*Deloitte & Touche LLP*
*Arlington, VA*

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8054

April 2015


U.S. Department of Commerce
*Penny Pritzker, Secretary*

National Institute of Standards and Technology
*Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director*

National Institute of Standards and Technology Internal Report 8054
62 pages (April 2015)

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8054



**Comments on this publication may be submitted to:**

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
**Email: nstic@nist.gov**

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.


## Abstract

Pilots are an integral part of the National Strategy for Trusted Identities in Cyberspace (NSTIC), issued by the White House in 2011 to encourage enhanced security, privacy, interoperability, and ease of use for online transactions. This document details summaries and outcomes of NSTIC pilots; in addition, it explores common themes in the pilots' work developing and operating innovative identity solutions.



## Keywords

Identity; security; privacy; interoperability; cooperative agreement; pilot; NSTIC; authentication; identity management; cybersecurity; information security.

## Acknowledgements

The following individuals participated in the preparation of this document: Barbara Cuthill, Mike Garcia, Jeremy Grant, Paul Grassi, and Naomi Lefkovitz. We would also like to acknowledge the efforts of all of the NSTIC pilot recipients whose hard work and perseverance continues to create the successes of the program, while exposing remaining challenges in the current state of the Identity Ecosystem.

## Audience

The purpose of this NISTIR is to summarize common themes from the NSTIC pilot work by highlighting overall successes catalyzed by the pilots, as well as suggesting areas where additional work could help to further develop the Identity Ecosystem. Organizations and individuals that seek to enhance the Identity Ecosystem may benefit from reading this NISTIR.

## Trademark Information and Company Information

This NISTIR comprises general discussion points relating to NSTIC pilot implementations. Any direct or indirect references to a specific pilot recipient's corporate capabilities or to any product or service offering is not intended to imply any endorsement or judgment by NIST but is used solely to illustrate common themes of the Pilots Program. The pilot recipients retain all of their trademark and company information.

# Table of Contents

# 1. Executive Summary

In 2011, President Obama signed the National Strategy for Trusted Identities in Cyberspace (NSTIC) to improve online transactions through the creation of an Identity Ecosystem. The Strategy calls for the private sector to "lead the development and implementation of this Identity Ecosystem," and for government to "partner with the private sector to ensure that the Identity Ecosystem implements all of the Guiding Principles."[1]

In support of this, the NSTIC National Program Office (NPO) established the NSTIC Pilots Cooperative Agreement Program (Pilots Program), focused on catalyzing a marketplace of identity solutions that adhere to the vision and principles in the NSTIC. The Pilots Program is an integral part of the implementation of the NSTIC; since 2012, the National Institute of Standards and Technology (NIST) has awarded approximately $30 million to 15 pilots.

These pilots have seeded the market with NSTIC-aligned identity solutions, engaging the healthcare, financial, education, retail, aerospace, and government sectors, among others. Observing the work of these pilots, the NSTIC NPO has identified several common themes in developing and operating innovative identity solutions. These fall into three general categories:

1. Market forces and relying party (RP) motivations;[2]
2. Emerging identity architectures and components; and
3. Standards and interoperability.

Among other important technical points, a number of pilots clarified the critical role of componentization of identity functions in establishing sustainable solutions: the identity market is made up of a variety of discrete functions (e.g., identity provider [IdP], RP, attribute provider [AP]), and identity proofing and credential issuance are often separated in identity architectures. The pilots recognized the importance of defining the functions within an architecture as opposed to the actors implementing the functions. They also revealed the challenges of managing a componentized architecture, since existing certification schemes don't always support componentization.

The pilots also faced similar challenges in their business transactions – especially when conveying the value proposition of identity solutions to relying parties. Generally, organizations outsource anything that isn't a core competency unless there's a significant risk to not doing this work themselves. The pilots found that RPs often didn't consider identity management a core competency,

[1] *National Strategy for Trusted Identities in Cyberspace – Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[2] An RP is an online service that relies on an external identity provider to authenticate a user.

but also struggled to assess the organizational risk of outsourcing it. The pilots found it necessary to present their solutions in a way that spoke to an organization's top line: the RP's ability to generate revenue and recruit and retain customers.

While this NISTIR focuses on the NSTIC Pilots Program, these pilots are only one pillar of implementing the NSTIC. The NPO also supports the development of an Identity Ecosystem Framework (IDEF) via the Identity Ecosystem Steering Group (IDESG), a private sector-led organization. Additionally, the NPO works with federal agencies to facilitate government's role as an early adopter of NSTIC-aligned identity solutions.[3]

The NSTIC pilots will continue to play a vital role in implementing the NSTIC by testing the commercial viability of various aspects of the Ecosystem and reporting back with lessons learned and by moving successful solutions into production. While some NSTIC pilots have advanced further than others, each has contributed to seeding the identity marketplace – by both successfully developing new technologies and models for online identity, and extracting valuable lessons learned. The work of these pilots lays a strong foundation for the future of the NSTIC Pilots Program and all organizations tackling online identity.

Moving forward, the NPO sees the continued importance of supporting the NSTIC Pilots Program to build upon the successes and address the challenges that the pilots have uncovered. The Pilots Program will evolve from addressing broad challenges to overcoming more specific gaps in the market, further catalyzing the marketplace and establishing a thriving and sustainable Identity Ecosystem.

[3] Read more about the government's role as an early adopter through their work with Federal Identity, Credential, and Access Management (FICAM) and Connect.gov: *FICAM*, http://www.idmanagement.gov; *Connect.gov*, http://www.connect.gov

# 2. Background

The National Strategy for Trusted Identities in Cyberspace (NSTIC), signed by President Obama in 2011, is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve online transactions.[4] The NSTIC vision is that individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. It describes four Guiding Principles (GPs) to which all identity solutions will adhere: (1) privacy-enhancing and voluntary, (2) secure and resilient, (3) interoperable, and (4) cost-effective and easy-to-use.

The NSTIC vision will be realized through the creation of an Identity Ecosystem: an online environment where individuals and organizations will be able to trust each other because they follow agreed-upon standards and policies to obtain and authenticate their digital identities. Implementation of the NSTIC has three major focus areas:

(1) Catalyzing a marketplace of identity solutions through the NSTIC pilots discussed in this document.
(2) Supporting the development of an Identity Ecosystem Framework (IDEF) via a private sector-led organization. This framework of standards and policies serves as a foundation for interoperability across the Ecosystem. The Identity Ecosystem Steering Group (IDESG) is a privately-led, non-profit organization which received a NIST grant to lead the framework development. NIST participates in the IDESG, along with 240 organizational and 120 individual members that span the academic, advocacy, government, and private sectors.
(3) Establishing the federal government as an early adopter of NSTIC-aligned identity solutions. Connect.gov - a hub-based federation solution – officially launched in a pilot phase in November 2014. It aims to ease the process by which agencies can accept federated credentials from both government and commercial identity providers (IdPs).

**NSTIC Pilots Program**

NIST launched the NSTIC Pilots Cooperative Agreement Program (Pilots Program) in 2012 to advance the NSTIC vision, objectives, and Guiding Principles by catalyzing a marketplace of NSTIC-aligned identity solutions that overcome barriers that have impeded development of the Identity Ecosystem.

[4] *National Strategy for Trusted Identities in Cyberspace – Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

Since the onset of the Pilots Program, NIST has awarded funding for four sets of NSTIC pilots through a competitive process – 15 pilots in total. The pilots are laying the groundwork for a vibrant new marketplace of identity solutions by developing and deploying technology, models, and frameworks that wouldn't otherwise exist in the marketplace. Additionally, they are informing the development of the IDEF within the IDESG.

The NSTIC pilots are funded as cooperative agreements, enabling a significant degree of collaboration between the NSTIC National Program Office (NPO) and the pilot recipients throughout the life of the grant. The pilots have been successful in their efforts to seed the marketplace with identity solutions; their work has led to a wide variety of technologies that facilitate stronger identity solutions for relying parties (RPs) across many communities. An RP is an online service that relies on an external IdP to authenticate a user. An RP may also use an attribute provider (AP) service to verify user identity attributes. The pilots have produced tangible benefits for the broad array of RPs participating in the pilots, and are bringing the importance of stronger, more convenient identity solutions to the attention of businesses and consumers alike. The purpose of this report is to provide a summary of the outcomes of the NSTIC Pilots Program to date and to illustrate common themes and considerations brought to light by the pilots' work.

**Selection of Pilots**

With each round of funding, NIST employs a two-step approach to select the NSTIC pilots. In the first step, interested applicants submit an abbreviated application describing the proposed project in no more than four pages. In the second step of selection, NIST narrows the field to the applicants that best align with program goals and invites them to submit full applications with detailed budget information, a technical proposal of no more than 25 pages (including in-depth information on the proposed technical solution, a schedule of milestones, etc.), letters of support from partners, and other items supporting the application. These finalists undergo a thorough review and evaluation process, and NIST ultimately selects those that have the greatest chance of advancing the NSTIC GPs and catalyzing a marketplace of identity solutions.

After selecting pilots, the NSTIC NPO continually monitors their performance and conducts formal evaluations on a quarterly basis. This provides regular opportunities to review strengths and accomplishments, to address challenges and changes in pilot timelines, and to make any adjustments to increase the likelihood of pilot success.

In this resource-constrained environment for pilot funding, the NPO uses a performance-based approach to make ongoing funding decisions based on actual pilot results. Annually, the NSTIC NPO measures pilots' progress against multiple factors – including their original proposals, established metrics, and mutually agreed-upon goals and objectives – to inform these performance-based funding decisions. Some pilots receive funding for multiple years because they

are continuously advancing and catalyzing the marketplace of identity solutions, while other pilots produce maximal value earlier in the project. Pairing performance evaluations of current pilots with a rigorous selection process for new ones, each year the NPO selects a full pilot portfolio with the potential to most effectively catalyze the marketplace.

## 2.1. Summary of first phase of NSTIC Pilots (FY2012)

In 2012, NIST received 186 abbreviated applications in response to the federal funding opportunity (FFO). Of 27 finalists, five were selected as pilots in the initial round of NSTIC cooperative agreements. These pilots were key to the IDESG in its nascent phases, by testing concepts in the marketplace and sharing their experiences to inform the development of the Identity Ecosystem. The remainder of this section provides a summary of each funded pilot.

***The Cross Sector Digital Identity Initiative (CSDII)***

**Recipient: The American Association of Motor Vehicle Administrators (AAMVA)**

AAMVA leads CSDII, a consortium of private industry and government partners formed to leverage in-person proofing at state departments of motor vehicles (DMVs) – done as part of the driver's license issuance process – to strengthen social login credentials held by consumers (existing logins from social networking and email providers such as Google and Facebook). Throughout the pilot, AAMVA has been responding to market needs by leveraging other remote and in-person identity proofing events, such as in-person proofing through healthcare providers.

In addition to AAMVA, the CSDII consortium includes the Commonwealth of Virginia Department of Motor Vehicles, CA Technologies, Microsoft, and Biometric Signature ID. The pilot focuses on healthcare applications and a state use case. The healthcare applications will enable patients and providers to easily and securely access health information with strong digital credentials. Additionally, the CSDII pilot will provide individuals with convenient online access to governmental services via Commonwealth of Virginia websites.

Outcomes:

- Developed a solution that innovatively binds identity proofing capabilities to social login credentials. For example, AAMVA brokers a process enabling individuals to link social logins to a set of verified attributes obtained through a prior in-person proofing visit to the Virginia Department of Motor Vehicles. Individuals can also link social logins to a 3rd party identity proofing solution via Experian or existing in-person proofing events through healthcare providers.
- Uses Microsoft's orchestration tool based on the U-Prove token technology to restrict the personal information accessible to RPs and all participant organizations (i.e., IdPs, APs) to only that required for a transaction. This privacy preserving technology offers the end users assurance regarding the ongoing privacy and security of their information.

- Established the CSDII Pilot Trust Framework and gained agreement among pilot participants (i.e., RPs, IdPs, APs, and companies providing remote proofing and identity infrastructure) on operational policies and practices, legal bylaws, and recommended participant practices. This approach streamlines the onboarding of additional states and other parties to the CSDII and saves the costs of developing and maintaining bilateral agreements. Currently, new participants are reviewing the CSDII Pilot Trust Framework to participate in the CSDII.
- Exposed the need for Virginia to pass specific legislation around identity, which informed House Bill 1562. Passed in 2015, the Electronic Identity Management Bill codifies the Commonwealth's approach to trust frameworks, standards, and liability.[5]

***The Attribute Exchange Network***

**Recipient: Criterion Systems, Inc.**

Criterion Systems, Inc., successfully deployed a user-centric online Attribute Exchange Network (AXN) that enables individuals to enhance their existing credentials (e.g., email, social network providers) for use in secure transactions. The AXN brings together multiple IdPs and APs, allowing individuals to manage their attribute data via a user-managed console. The AXN creates a modular way for online service providers to help individuals "build" a strong credential for enhanced-trust applications by linking together multiple claims (e.g., name, street address, age) already known by APs in the marketplace. As an example of how Criterion worked with a number of organizations across sectors, it supported first responders with the Department of Homeland Security (DHS), and customers of a Fortune 100 company and Broadridge Financial Services – the leading provider of investor communications and technology-driven solutions for wealth management, asset management, and capital markets firms.

IdPs included Google, Verizon, Symantec, AOL, Facebook, LinkedIn, and Amazon. APs included LexisNexis, Experian, Equifax, and PacificEast.

Outcomes:

- Successfully piloted the AXN solution at Broadridge, enabling customers to securely access mobile delivery of financial services content, bill presentment, and bill pay. Criterion launched with the new Broadridge/Pitney Bowes joint venture, offering secure digital delivery to 140 million customers.
- Successfully piloted with a Fortune 100 company, enabling them to access corporate data by verifying the attributes of company partners who

[5] *HB 1562 Electronic Identity Management; Standards, Liability*, March 2015, http://lis.virginia.gov/cgi-bin/legp604.exe?ses=151&typ=bil&val=hb1562

provided external credentials. This facilitated the sharing of sensitive company data among internal and external partners in a way that preserved privacy, security, and efficiency.

- In partnership with DHS, enabled over 1100 transactions, which support first responders in more easily accessing the National Incident Command Service to efficiently and securely share information.
- Worked with the U.S. Census Bureau to test an ability for respondents to the upcoming 2016 American Household Survey to electronically verify their personal information and complete the survey online. This approach could result in potentially significant cost savings in survey administration.

***Advancing Commercial Participation in the NSTIC Ecosystem***

**Recipient: Daon, Inc.**

Daon adapted its IdentityX authentication technology to align with the NSTIC principles by converting a proprietary solution to a federated, interoperable, standards-based (Security Assertion Markup Language [SAML] and Open ID Connect [OIDC]) solution offering strong authentication in a manner that improves both security and usability.[6,7] Daon's IdentityX solution provides multifactor authentication (MFA) on the iOS and Android platforms with the ability to selectively combine a variety of traditional and non-traditional authentication methods of varying strength – voice and face biometrics, device authentication, password, PIN, one-time password, and location – depending on the risk level of the transaction and the choice of the customer.

A diverse group of RPs have brought high assurance credentials to a wider audience by piloting this solution, including AARP, Purdue University, and the American Association of Airport Executives (AAAE). Daon also worked with the Kantara Initiative and FICAM's Trust Framework Solutions (TFS), the federated identity framework for the U.S. Federal Government.[8] TFS includes guidance, processes, and supporting infrastructure to enable secure and streamlined citizen and business facing online service delivery.[9]

---

[6] *Security Assertion Markup Language (SAML),* https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[7] *OpenID Connect (OIDC),* http://openid.net/connect/

[8] Kantara Initiative is a private organization that provides strategic vision and real world innovation for the digital identity transformation.
*Kantara Initiative,* https://kantarainitiative.org

[9] In federated identity, the identity provider of your choice "vouches" for you at other sites.

Outcomes:

- Through a pilot with AARP, enabled members to securely access personal health information using a reusable interoperable credential, with MFA using facial and voice biometric recognition.[10]
- Provided lessons learned in using strong MFA technology that informed the United Services Automobile Association (USAA) in launching convenient and effective mobile account access for over 150 000 of its members through Daon's facial and voice recognition technology.
- Will enable individuals to securely access results of their FBI criminal history records check through AAAE, providing them with the ability to verify and correct information revealed in background investigation reports. Production is set to begin in 2015.
- Gave students secure access to online coursework and exams through a pilot at Purdue University, enabling institutions to place greater trust in the identity of students completing work online.
- Drove the development of key product certification considerations for the Identity Ecosystem, including the need for more componentized certification processes and flexibilty in assessments to accommodate evolving and innovative technologies. This work highlighted the need for trust framework providers (TFPs) adopted under TFS to update their trust frameworks to accommodate a more componentized architecture.[11]

***Patient Coordination of Care/Zero-Knowledge Identity and Privacy Protection Service***

**Recipient: Resilient Network Systems, Inc.**

Resilient Network Systems (RNS) deployed a decentralized authentication system – based on a network of IdPs, APs, and RPs – that limits the distribution of personal information. The RNS pilot included the following partners: the National eHealth Collaborative, the American Medical Association, Authentify, Knowledge Factor, and the National Laboratory of Education Transformation.

The above partners executed use cases in the healthcare and education sectors. This work enabled San Diego Beacon (a healthcare provider) and California public schools to operationalize identity solutions across their systems, more securely accessing sensitive information.

[10] *Everybody Needs Identity*, NSTIC Notes, November 2014, http://nstic.blogs.govdelivery.com/2014/11/28/everybody-needs-identity/

[11] *TFS Framework Solutions,* http://www.idmanagement.gov/trust-framework-solutions

Outcomes:

- The RNS pilot architecture evolved into a network for information sharing with the Northern California Regional Intelligence Center (NCRIC), enabling the transfer of highly secure information. Selected as a top 30 finalist for the American Council for Technology - Industry Advisory Council (ACT-IAC) Igniting Innovation awards as a result of this work.[12]
- Piloted the RNS platform with the San Diego and Gorge Health Connects, enabling the sharing of patient health information between these health information exchanges by securely and effectively verifying doctor and staff identities. This opportunity for secure and convenient collaboration ensures accuracy of data, which is imperative in saving hospitals and patients valuable resources, while reducing the likelihood of misdiagnoses.
- Deployed the RNS pilot architecture in California's Pajaro Valley Unified School District to further engage parents and guardians in their children's academics, by verifying their relationship to their children and providing them secure access to these students' information online.
- In partnership with Kantara, analyzed individual functions, challenging the conventional monolithic viewpoint of trust frameworks to address decomponentized identity architectures.

***Scaling Privacy and Multi-Factor Authentication***

**Recipient: University Corporation for Advanced Internet Development (UCAID or Internet2)**

Internet2 is developing tools and initiatives to advance privacy-enhancing technology for the Identity Ecosystem. Their work includes deploying smartphone-based MFA across three major university campuses, establishing a collaborative group to accelerate the adoption of MFA across universities, developing a user-centric privacy management tool, and assessing the current state of anonymous credential technologies.

Outcomes:

- This pilot provided funds for the Massachusetts Institute of Technology, the University of Texas, and the University of Utah to deploy MFA, and create a forum for over 50 university campuses and other organizations – representing more than a million users – to establish and improve deployment of MFA technologies.

[12] *Better Government IT*, The American Council for Technology and Industry Advisory Council, 2011, http://www.kms.ijis.org/db/attachments/procurementinnovation/115/1/ACT-IAC%20IT%20Summary%20Report.pdf

- Developed and made publicly available a simplified MFA enablement of Shibboleth IdPs. This work also catalyzed adoption in the research and education community; currently, over 140 universities have begun to deploy a variety of MFA technologies. By addressing MFA management at the enterprise level, this work has provided a vital missing piece for scaling MFA.
- Identified key technical and business barriers to the widespread adoption of anonymous credential technologies. Published a white paper outlining the steps that could be taken to resolve these barriers.[13]
- Developed an open-source privacy manager called PrivacyLens, driven by research at Carnegie Mellon into user preferences for the management of their personal information. PrivacyLens gives users effective methods for transparent, granular, consent-based release of personal information or attributes associated with their credentials.
- Developed and published the "Periodic Table of Trust Elements" that advances the concept of componentizing the elements of trust.[14] The Georgia Tech Research Institute (GTRI) Year 2 project is further elaborating on this concept, helping participants in the Identity Ecosystem to understand the equivalency – across multiple communities – of components of trust that they have established. This ultimately reduces an organization's overhead and the barriers to participating in multiple communities.

[13] See *Appendix 5.3: White Papers*
[14] *A Periodic Table of Trust Elements*, Internet2, 2013, https://spaces.internet2.edu/download/attachments/33099874/PeriodicTable_131108.pdf?version=1&modificationDate=1385562509851&api=v2

## 2.2. Summary of second phase of NSTIC Pilots (FY2013)

The 2013 NSTIC pilots built upon the successes and lessons learned from the previous round of awardees. These pilots leveraged new componentized identity architecture models with innovative business models to service new communities of interest, while further developing and refining legal and governance structures that are necessary for success. In 2013, NIST received 63 abbreviated proposals, and invited 13 to submit finalist proposals before choosing the recipients of NSTIC cooperative agreements. NIST funded five pilot projects, four of which are explained below. The fifth pilot award, received by Exponent, Inc., was mutually terminated after changes in a key team member's corporate strategy introduced an unanticipated risk for Exponent's ability to execute on its proposal.

### *Scaling Interoperable Trust through a Trustmark Marketplace*

**Recipient: Georgia Tech Research Institute (GTRI)**

GTRI is tackling a significant barrier to adoption within an Identity Ecosystem: the difficulty in enabling trust and interoperability across multiple communities of interest (COIs) and trust frameworks. In simple terms: how can IdPs, RPs, and end users trust each other in a way that's scalable across the Identity Ecosystem?

While different COIs often have their own specific rules to enable trust, there are also certain requirements that are consistent across communities. GTRI is focusing on identifying these common rules by componentizing the many parts of trust frameworks into individual trustmarks.[15] For instance, two COIs may have individual sets of requirements, but GTRI can analyze these and componentize them into discrete sets for trustmarks. The hypothesis is that many of these trustmarks will be common across the two COIs. By identifying the commonalities and differences between two COIs, it becomes simpler for a participant of one COI to identify what it needs to do to become a member the other.

Componentizing and clearly defining trustmarks for specific policies may also allow website owners, TFPs, and individual internet users to more easily understand the technical, business, security, and privacy requirements and policies of the websites with which they interact.

Outcomes:

- Developed a trustmark framework to facilitate greater trust and interoperability of trustmarks across the Identity Ecosystem.

[15] *The Trustmark Concept,* GTRI, 2014, https://trustmark.gtri.gatech.edu/concept/#how-trustmarks-can-help-fix-what-is-wrong

- Developed over 60 unique trustmark definitions by analyzing and decomposing National Identity Exchange Federation (NIEF) and FICAM trust and interoperability requirements, encouraging interoperability across COIs.[16] Currently undergoing additional assessments on NIEF members.
- Issued over 90 trustmarks to organizations in NIEF, which currently serve law enforcement agencies across the United States.
- Developing publicly available software tools for defining trustmarks, defining trust criteria in terms of trustmarks, performing assessments for trustmark issuance, managing the trustmark issuance lifecycle, and facilitating the binding and use of trustmarks by operational systems.

***Catalyzing the market with NSTIC-aligned, FICAM-approved Credentials***
**Recipient: ID.me, Inc.**

Through the NSTIC Pilots Program, ID.me has enhanced its existing identity solutions to further align to the NSTIC and accelerate the adoption of NSTIC-aligned credentials across commercial and government organizations. ID.me's identity attribute verification and credentialing enables registered users to voluntarily assert validated attributes about themselves while also accessing sensitive information and services online in a privacy-enhancing, secure, and efficient manner. ID.me currently works with retail organizations, financial institutions, and government agencies, and will soon expand to the healthcare sector.

ID.me began as TroopID, enabling America's service members, veterans, and their families to verify their military affiliation online across a network of organizations that provides discounts and benefits in recognition of their service. They've expanded to now verify the affiliations of first responders, students, and teachers. Today, close to one million consumers use ID.me credentials to access discounts and benefits online.

Outcomes:

- Since the pilot began, ID.me has more than tripled its membership, enabling an additional 500 000 service members, veterans, teachers, first responders, and students to access discounts and benefits online from more than 200 commercial organizations (e.g., Sears, Sea World, Under Armour), government entities, and non-profit organizations without having to share sensitive documents or personally identifiable information each time they want to prove eligibility. Under the pilot, ID.me has increased the number of RPs using its services by 167%.

[16] *Trustmark Definitions,* GTRI, 2014, https://trustmark.gtri.gatech.edu/operational-pilot/trustmark-definitions/

- Measured the impact of adopting federated solutions by their RPs to demonstrate revenue generated by trusted identity solutions, and published the results. As an example of this value, ID.me drove over 30% revenue growth in Under Armour's military and first responder market segment. ID.me also expanded Under Armour's customer base: 70% of those who used ID.me credentials at checkout since November 2012 were first-time customers to Under Armour.[17]
- Successfully certified by Kantara as a FICAM TFS-approved credential service provider, allowing ID.me to provide federated logon for government services. ID.me and Verizon were the two credential service providers procured by the General Services Administration (GSA) to provide credentials for levels of assurance (LoA) 1, 2, and 3 transactions through the Connect.gov pilot phase.

### *The Minors Trust Framework & The PRIVO Parent's Hub: Parental Consent at Internet Scale*

**Recipient: Privacy Vaults Online, Inc. (PRIVO)**

Privacy Vaults Online (PRIVO) is piloting a solution that improves the way parents and guardians establish and leverage their digital identities to authorize their children's interaction with online services in order to comply with the Children's Online Privacy Protection Act (COPPA). COPPA is a federal law that aims to regulate websites, mobile applications, games, and other online services that collect information from children under the age of thirteen by detailing what they must include in a privacy policy or direct notice and when to seek consent from a parent or guardian.

Prior to the award of this NSTIC pilot, the Federal Trade Commission (FTC) approved PRIVO as an identity and permission management solution provider; PRIVO was also granted COPPA Safe Harbor status. Companies with digital properties who partner with PRIVO to become COPPA compliant are first subject to the procedures of the safe harbor program and are therefore shielded from FTC enforcement. With this pilot, PRIVO enhanced its safe harbor offering to expand on its policy and technology solution to make it interoperable and more robust, secure, privacy enhancing, and easy to use for parents, children, and online service providers.

Outcomes:

- Enabled parents to more easily manage their children's access to COPPA-compliant digital properties. Parents can now use a single portal to learn about the privacy practices of RPs that use PRIVO's solutions, then provide and revoke consent for sharing their children's personal

[17] See *Appendix 5.3: White Papers*

information to these applications and websites. More than 247 000 accounts are under management by PRIVO, thus providing a unique location for parents to assert and implement their online parental rights. The solution gives parents more granular view and control over which specific attributes get shared with which RPs on a feature by feature basis.

- Enabled IdP services with the interoperable standardized authentication protocols SAML and OIDC to enable a smooth user experience across digital properties.
- Implemented services that facilitate children's access to websites, mobile applications, games, and other online services without the need for the collection of children's personally identifiable information.
- Developed a Minors Trust Framework that integrates the NSTIC principles with the requirements from COPPA to elevate the level of trust across participating organizations. This framework's governance will be transitioning to an independent third-party in 2015, with the goal of establishing broad and widespread adoption. Organizations from the public and private sectors – including technology vendors, global certification groups, and service providers – are currently reviewing the MTF and expressing interest in adoption.

### *Trust Framework Development Guidance for Small and Medium-sized Businesses and Financial Sectors Pilots*

**Recipient: Transglobal Secure Collaboration Program, Inc. (TSCP)**

The TSCP NSTIC pilot is focused on broadening the reach of its core operating rules to incorporate credentials with all levels of assurance, for both public key infrastructure (PKI) and non-PKI environments, and across multiple sectors. Prior to this pilot, TSCP had established a set of core operating rules that enabled firms in the aerospace and defense sector to trust each other's high assurance credentials, as well as the credentials of federal agencies.

The goals of the pilot project are to create a trust framework that allows employees of participating companies to use their existing credentials to securely assert their identities and log into retirement accounts at a brokerage firm and other financial institutions, rather than maintaining separate credentials for these sites.

Outcomes:

- Proved the technical capability of using strong corporate credentials to access personal 401k accounts by piloting corporate-provided PIV-I credentials with Fidelity's Net Benefits application.

- Built on the existing TSCP core operating rules to align with FICAM LoA 1 through 3 and to include additional guidance for comparability, facilitating identity federation across the financial, aerospace, and defense industries.
- Developed the Trust Framework Development Guide, to assist organizations across multiple sectors in developing their own trust frameworks that extend from LoA 1 through 4, align with NSTIC Guiding Principles, and include requirements from an array of industries and sectors.
- Highlighted challenges around large financial organizations adopting federated identity solutions.

## 2.3. Summary of NSTIC State Pilots (FY2013)

In 2013, the NSTIC NPO released an FFO targeted specifically at state governments, due to the vital role that states play in the Identity Ecosystem both as potential IdPs, and as RPs. These state programs did not receive NSTIC NPO funding; rather, the funding came from the Office of Management and Budget's (OMB) Partnership Fund for Program Integrity Innovation, which was established by Congress in 2010 to help federal agencies and state governments work together to find smarter ways to meet the demands of citizens and act as responsible stewards of taxpayer resources.[18] OMB administered the Partnership Fund in consultation with the Collaborative Forum, which included state representatives and other stakeholders. The Partnership Fund enabled federal, state, local, and tribal governments to pilot innovative ideas for improving state delivery of federal assistance programs. Out of six applicants, two state governments were chosen as pilots in 2013. Since these states are funded and managed separately from the above pilots, their timelines differ. They are still in the early phases of their projects, so the summaries below do not include outcomes. The state pilots collaborate with the NPO and the other pilots and helped to inform the common themes introduced later in this paper.

### *Cross-Agency User Validation*

**Recipient: Commonwealth of Pennsylvania**

The Commonwealth of Pennsylvania is deploying a state identity exchange that enables individuals to obtain a Keystone ID through two identity proofing options and use this credential to conduct online transactions across the Commonwealth. The initial phase will pilot with a number of participating agencies including the Department of Human Services and Pennsylvania Human Relations Commission. With this technology, citizens are able to register just once to access a variety of services, eliminating the need to create multiple accounts and to validate their identity multiple times. If successful, these higher security accounts will allow new types of online transactions, increasing convenience while also helping the state reduce fraud.

### *Michigan Department of Human Services Identity Authentication Project*

**Recipient: Michigan Department of Human Services**

The Michigan Department of Human Services is piloting the use of secure, privacy-enhancing online identity verification and authentication solutions with MiBridges, Michigan's integrated eligibility system that supports online enrollment and registration for over 2.3 million Michigan residents seeking public assistance. The pilot project, in partnership with LexisNexis, aims to help eliminate barriers citizens face in accessing benefits and services by streamlining the identity

[18] *The Partnership Fund for Program Integrity Innovation*, http://partner4solutions.gov

proofing part of the applications process, while also reducing fraud and improper payments. The pilot project is also evaluating how residents can more securely access their private information using MFA solutions. The outcomes of this pilot will inform the larger enterprise architecture identity verification and authentication solutions for Michigan state government.

## 2.4. Summary of third phase of NSTIC Pilots (FY2014)

In 2014, NIST received 40 abbreviated proposals and invited eight to submit finalist proposals before choosing three recipients of NSTIC cooperative agreements. Like the state pilots, these three pilots are early in their projects and do not have outcomes listed. These projects did not inform the compilation of common themes in this document. As part of the overall program, these three pilots, as in previous years, augment the current portfolio of pilots and develop areas that were not addressed in past years.

***Digital Identity Fraud Alert System***

**Recipient: Confyrm**

Confyrm will demonstrate ways to minimize loss when attackers create fake accounts or take over online accounts. A key barrier to federated identity is the concern that accounts used in identity solutions may not be legitimate or in the control of their rightful owner. Account compromises and the subsequent misuse of identity can result in the destruction of personal information, damage to individual reputations, and financial loss. Confyrm will demonstrate how a shared signals model can mitigate the impact of account takeovers and fake accounts through early fraud detection and notification, with special emphasis on consumer privacy. Aligning with the NSTIC Guiding Principles, this solution enables individuals and organizations to experience improved trust and confidence in identities online.

***Enabling Mobile-based Identity and Access Management Technologies***

**Recipient: GSMA**

GSMA has partnered with four of America's major mobile network operators – AT&T, Sprint, T-Mobile USA, and Verizon – to pilot a common approach to enable consumers and businesses to use mobile devices for secure, privacy-enhancing identity and access management. GSMA's global Mobile Connect Initiative is the foundation for the pilot; the initiative will be augmented in the United States to align with the NSTIC. By allowing any organization to easily accept identity solutions from any of the major operators, the solution would reduce a significant barrier to online service providers accepting mobile-based credentials. GSMA also will tackle user interface, user experience, security, and privacy challenges, with a focus on creating an easy-to-use solution for consumers.

### *Proving the Efficacy of an Electronic Identity in Online Transactions by Leveraging the Trust of a State Driver License Vetting Process*

**Recipient: MorphoTrust USA**

MorphoTrust will demonstrate how the trust placed in state-issued driver licenses as a primary proof-of-identity document can be extended into the online world, enabling secure transactions and delivery of state services to citizens. The pilot will leverage identity proofing done by the North Carolina Department of Transportation to create a digital credential for applicants to Food and Nutrition Services (FNS) programs in the North Carolina Department of Health and Human Services. This solution aims to eliminate the need for people to appear in person to apply for FNS benefits, reducing costs to the state while providing applicants with faster, easier access to benefits.

# 3. Pilot Themes

Many of the NSTIC pilots faced similar issues, thus highlighting the common challenges in catalyzing and operating in a marketplace of identity solutions. This section contains, from the NPO's perspective, the pilots' experiences, separated into three general categories:

1. Market forces and RP motivations;
2. Emerging identity architectures and components; and
3. Standards and interoperability.

The NSTIC NPO recognizes the need to respect pilots' sensitive business information, while ensuring that the pilots' general experiences are publicly available to inform the work of other organizations developing identity solutions. Thus, while these common themes originate from real-world pilot experiences, the themes section aggregates multiple pilots' feedback. These common themes are observations of the pilots' experiences overcoming barriers in the market and implementing the NSTIC.

As recipients of NIST cooperative agreement funding, the pilots regularly collaborate with the NPO, beginning with a kickoff meeting, followed by a preliminary design review. During the design review, the pilot explains how its project team will accomplish the goals in its proposal. This is an opportunity to collaborate with the NPO on architectures, technologies, and policies to ensure that the project aligns with the GPs and is achievable within the parameters agreed to in the cooperative agreement. The pilots also participate in an NPO-facilitated cross-pilot collaboration working group that identifies and works through key challenges.

Members of the pilot teams also actively engage in the IDESG by providing input and serving in leadership roles. They have been very effective in advancing the organization's work by informing and testing materials produced by the IDESG. For example, many of the pilots used the IDESG Privacy Evaluation Methodology to evaluate their organizational privacy risk. They then provided feedback to the IDESG on improving this document for other organizations' use. The pilots also provided formal commentary on the requirements catalog under development in the IDESG, helping to refine these requirements based on their experiences. Additionally, they identified the gap in standards around knowledge-based authentication discussed in the *Standards and Interoperability* section below. The pilots meet regularly with the NPO to discuss these various roles and responsibilities both as individual organizations and as a group in the collaboration working group.[19]

[19] See *Appendix 5.4: Pilot Contributions to the IDESG*

The pilots accomplish the goal of catalyzing a marketplace of identity solutions in a number of ways; for example, they spread the importance of stronger identity solutions, and offer their experiences as lessons learned to other organizations with similar goals. Moreover, the NPO and the IDESG generally learn as much or more from pilots' challenges as their successes – when pilots have struggled, it is because they have unearthed a new barrier or challenge that needs to be addressed.

More plainly, while each pilot stands on its own merits, the NSTIC Pilots Program aims to catalyze a marketplace, not a single solution. To that end, the impact of the full pilot portfolio is far greater than that of the individual pilots. By funding a diverse set of pilots providing different technologies, infrastructure, and policy approaches, the Pilots Program seeds an array of solutions that "stress tests" and contributes to a more robust identity marketplace in which users are the ultimate arbiters of adopted solutions.

The following sections describe the collective work of the NSTIC pilots by organizing feedback and lessons learned into themes that reflect pilots' experiences in deploying innovative identity solutions.

## 3.1. Market Forces and RP Motivations

Many of the pilots' experiences relate to general market forces and RP motivations. As one example, pilot experiences indicate that enterprise deployments of MFA are increasing in number, but such an increase does not seem as evident for consumer applications.[20] In addition, many MFA deployments are not federated. The NSTIC envisions technology, infrastructure, and policy solutions that facilitate the use of strong authentication in a federated manner. Efforts to increase the adoption of strong authentication technologies will be of limited success if users replace dozens of username and passwords with dozens of different strong authentication technologies. This need for federation was a primary motivation for creating the NSTIC Pilots Program.

Many pilots have had difficulty communicating the value proposition of federated identity approaches to RPs. Pilots determined that it required a great deal of education, since most organizations were unfamiliar with the concept. Pilots had to first educate RPs on the principles of federated identity before being able to effectively communicate the benefits of their specific solutions. In addition to the need to educate potential RPs on these concepts, the pilots determined that they required a thorough understanding of RPs' business interests – and customers' desires – to effectively encourage them to adopt these new technologies. This process often took much longer than anticipated as RPs did not buy in as readily as hoped, instead maintaining a higher-than expected degree of risk aversion toward new processes.

The pilots found that a focus on the business benefits or the mitigation of "pain points" of an organization tended to be more successful in fostering interest in adoption than the mitigation of security or privacy risks. **RPs were particularly interested in business drivers that increased revenue.** While an RP's IT security division played a critical role in advancing the technology solution to production, discussion of the business drivers brought the business champions to the table to engage the RP in federated solutions. Several pilots have been working to record the tangible impact of these new technologies to enable conversations with potential RPs about the financial benefits of federated solutions, including statistics that clearly demonstrate revenue growth, increased sales, and other measurable effects of pilot-RP partnerships. Pilots found that a particularly important factor in increasing RPs' revenue was the strengthening and expanding of an organization's customer base.

---

[20] 37 percent of organizations use MFA for a majority of employees – up from 30 percent in 2013. By 2016, 56 percent of organizations expect the majority of users to rely on multi-factor authentication. Based on a survey of over 350 corporate senior IT decision-makers from around the world.
*2014 Authentication Survey*, SafeNet, Inc., 2014, http://www.safenet-inc.com/resources/data-protection/2014-authentication-survey-executive-summary/.

**Potential RPs seemed concerned that altering their authentication technology, and thus how they interacted with their customers, would lead to customer friction and drop-off, and therefore preferred to retain control over the customer relationship and user experience.** Pilots focused on minimizing this potential friction to enable expansion of an RP's customer base, ultimately increasing revenue.

Several pilots focused on promoting the increase in customer satisfaction that could arise from the adoption of federated solutions. Since many RPs were focused on their customer satisfaction above security mitigation, this was an important point to stress in conversations with these organizations. **Pilots found that RPs were interested in technology enhancements that streamlined authentication processes, and ultimately increased an organization's user base and revenue.**

**Some pilots enabled a more frictionless experience for the end user by enabling a strengthened social login credential**, such as a pre-existing username and password from a social networking site. Customers used this credential along with additional factors – such as out of band communication or an identity-proofing event – as additional controls to enhance the strength of a credential. This resulted in credentials that were strong enough for secure transactions while convenient enough for individuals to easily use.

When struggling with RP adoption, some **pilots reached out directly to users to inform them about why they were being asked to switch to new technology and the benefits they would reap**. Once the users understood the value proposition – such as single sign-on or new functionality at the RP site due to stronger identity proofed credentials – user adoption at the RPs increased.

A few pilots addressed the issue of customer friction by approaching RPs with an extensive set of previously enrolled users, which appealed to RPs because it was an opportunity for RPs to become visible to, and acquire, new customers. Rather than requiring RPs to rely on current customers to actively transition to new technology and register on a site, these pilots provided RPs with individuals who had already completed the IdP registration process. **Certain pilots focused on specific user populations (e.g., students, teachers, veterans, parents), expanding a potential RP's reach by bringing in an entirely new community of customers**.

**Pilots observed that focusing on the benefits of an interoperable credential to customers was less effective when working with *large* organizations.** Some of the larger potential RPs made it clear that they had the resources to "do things themselves" and they didn't need to outsource identity management. They also expressed concern that the use of federated credentials might enable competition to learn of, and potentially share, customer lists. In these cases, a discussion of federated external credentials was less productive than a

conversation about how federation provides customers with choices while strengthening the overall Ecosystem.

To recruit customers, a couple of pilots focused on **enabling individuals to establish monetary benefits, such as discounts**, using their identity attributes. Individuals were able to verify their affiliations online across a network of RPs. This model offered tangible benefits to individuals, resulting in an increased user base for the RPs.

Several pilots observed that, as organizations review their privacy policies, legal concerns about the potential liabilities often lead to the inclusion of legal language designed to mitigate organizational risk. As this language tends to be unapproachable to users, privacy policies often become a poor venue for clear communication about privacy with individuals. **To resolve this issue, some pilots attempted to create new "plain language" approaches for communication with customers about privacy.** However, this remains for the pilots - and the wider world of information technology - a difficult challenge to overcome.

The pilots had to engage RPs in adopting stronger authentication and accepting interoperable credentials, while communicating the importance of these technologies to the RPs and their customers. **The hope is that this education will shorten the sales cycle as organizations become increasingly familiar with federated identity approaches.** The pilots also began to develop extensive bases of enrolled users to increase the incentive for RPs to use their services and to mitigate concerns about existing customer friction. In this way, the pilots are seeding the marketplace with federated solutions, instilling an understanding of strong authentication's value both in RPs and consumers.

## 3.2 Emerging Identity Architectures and Components

One of the most common threads in the NSTIC pilots was the emergence of new identity architectures and components, resulting in an early challenge with a lack of common industry terminology. An NPO blog on pilot terminology described the terms that pilots typically use and how they relate to the terminology from programs such as FICAM.[21] A second NPO blog discussed the emergence of a functional model for identity solutions.[22] Mapping this simple model to the pilots' approaches showed that even across the diverse technologies and capabilities of the pilots, **only a few identity functions are necessary to execute a wide range of identity use cases**. This analysis led to clarifying the core functional components in identity architectures and directly contributed to the functional model of the IDESG – a critical part of the IDEF.

### *3.2.1. Componentization Trends*

Early identity systems – often built for government applications – considered identity proofing and credential issuance as a single operation. The pilots' efforts demonstrated that these may often be separated within an identity architecture. This functional decomposition has been driven largely by vendor specialization and commercial forces, and provides additional architectural flexibility for alignment with the GPs. Such an architectural capability has been recognized by TFPs – including those adopted by FICAM – although it has not yet been fully incorporated into their certification scheme. Thus, a key challenge for pilots was the possibility that their architectures were not supported under the existing certification schemes. A coordinated response by the current FICAM adopted TFPs - Kantara, InCommon, and SAFE-BioPharma - clarified their views on the componentization approach in hopes of aligning government needs and industry practices.[23,24,25]

The functional model blog also noted that **defining functions within an architecture is typically more meaningful to system analysis than defining the actors that are implementing the functions**. For example, in several pilots, RPs wanted to rely on 3rd party services to strongly authenticate a user, but wished to retain their internal identity proofing services. This came down to a requirement or desire for the RPs to know their customers; the RP in this case also served as an IdP. These changing trends in approaches to identity require

---

[21] *NSTIC Pilot Common Considerations: 1- Terminology*, NSTIC Notes, April 2013, http://nstic.blogs.govdelivery.com/2013/04/12/nstic-pilot-common-considerations-1-terminology/

[22] *NSTIC Pilot Common Considerations 5: An Identity Ecosystem Functional Model for the Modern Market*, NSTIC Notes, August 2013, http://nstic.blogs.govdelivery.com/2013/08/02/nstic-pilot-common-considerations-5-an-identity-ecosystem-functional-model-for-the-modern-market-2/

[23] *InCommon*, https://www.incommon.org

[24] *SAFE-BioPharma Association*, http://www.safe-biopharma.org

[25] *IAWG Meeting Minutes 2014-11-20*, Kantara Initiative, November 2014, http://kantarainitiative.org/confluence/display/idassurance/IAWG+Meeting+Minutes+2014-11-20

full analysis of the binding mechanisms between the functions. This analysis of binding is increasingly important when several components are tied together, as the overall **credential strength is dependent on all elements within the "chain of trust."** This discussion is consistent with the "low water mark" discussion in NIST Special Publication (SP) 800-63-2, *Electronic Authentication Guidance*.[26]

### *3.2.2. Intermediary Components*

In several pilots, **an intermediary component was used as an operational layer between IdPs, APs, and RPs**. These intermediary components were, in some cases, pass-through transactional layers to simplify integration. In other cases they processed transactions in accordance with policy, serving as orchestration layers between identity services and RPs. Pilots also leveraged the intermediaries to increase the level of confidence that they had in an individual, using additional factors or attributes either on a transactional basis or to permanently step up the identity proofing. Several example architectures are shown on the next two pages in *Figure 1*.

The pilots varied in how they designed their architecture around intermediaries. One architecture was a hub and spoke model managed by a single entity. Another was componentized but in the cloud and operated by a single entity. A different componentized intermediary solution was in the cloud with the management of the multiple components separated by policy and allowed for control by multiple organizations. A fourth configuration relied upon the distribution of all components to the end-points for management. Several challenges arose from these different configurations. For example, **while distributed systems offered the potential of privacy preserving characteristics, scalability was challenging, and the end-point organizations (such as IdPs and APs) weren't always prepared to manage and control the required functional components**.

With intermediaries orchestrating various authentication and identity proofing functions, it is critical to consider user interface flow, consent flow, redress, and the principles of anonymity, unobservability, and unlinkability. In alignment with broader technological maturity, the pilots demonstrated some progress toward advanced privacy preserving technologies, such as zero knowledge protocols; however, they highlighted that many challenges remain due to scalability challenges, business tradeoffs, and immaturity of technology components. To address privacy challenges, **the pilots tended to implement a combination of policies and standard cryptographic methods while also exploring Personal Data Store (PDS) structures to manage individuals' access to personal data on an identity hub or elsewhere within an infrastructure**.

[26] *NIST Special Publication 800-63-2: Electronic Authentication Guideline,* NIST, August 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

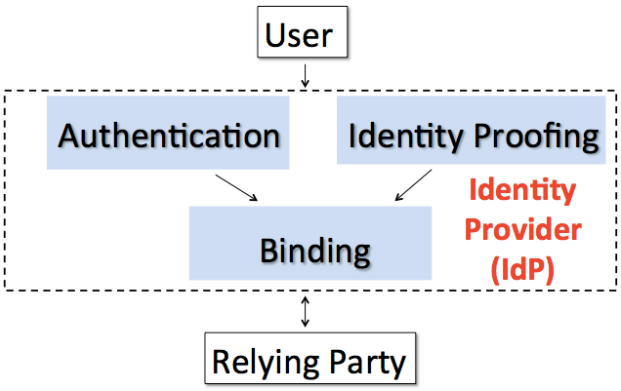


**Figure 1(a):** "Classic" IDP model, in which one provider delivers both identity proofing and authentication; thus, binding is inherent in the service. This is the basis for existing certification schemes (e.g., those adopted under the FICAM TFP Adoption Process), but the terminology used there for IdP is Credential Service Provider (see footnotes 21 and 22 for more details).

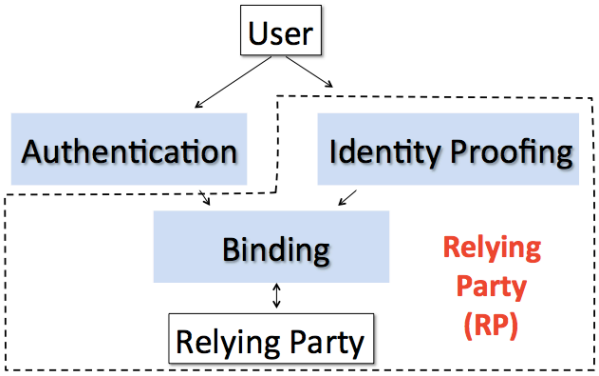


**Figure 1(b):** Each RP performs its own identity proofing and maintains the binding to the authentication service used. Several pilots expected to provide a full IdP service; after discussions with the RPs, it **became clear that some RPs wanted to support their own identity proofing**.

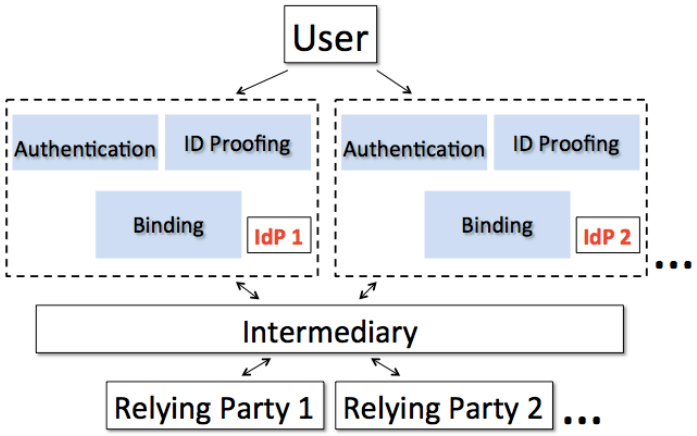


**Figure 1(c):** Intermediary produces "blind" operations between the IdP and the RP. This **allows RPs to interface with a number of IdPs without the effort and cost of integrating each of them.** This formed the basis for several of the pilots' architectures. Architectures with such intermediary layers can also be used to render the operations between participants blind – in this case, the IdPs and the RPs don't know who is performing an authentication or transaction, respectively.

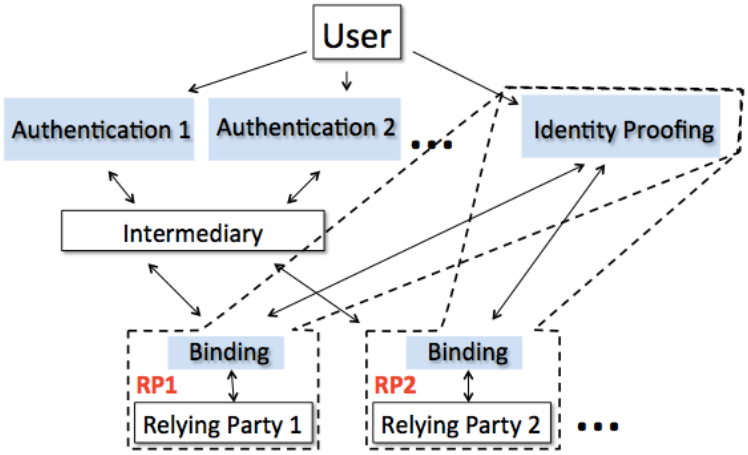


**Figure 1(d):** Intermediary is used to provide an abstraction to a number of different authentication means, but each relying party still performs its own identity proofing. This ability for RPs to perform identity proofing allows them to either "know their customer" in accordance with legislative requirements, or to use compensating factors to enhance the authentication process prior to the provision of a service.

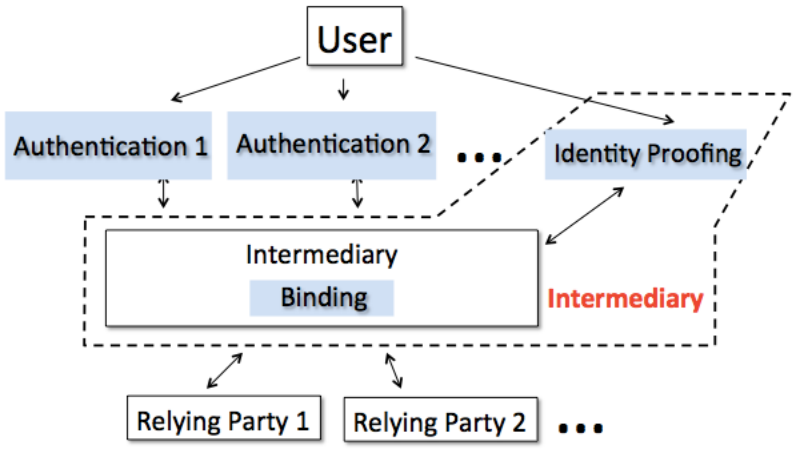


**Figure 1(e):** Intermediary performs identity proofing and binding. This is applicable when an intermediary wishes to offer a identity services in an "a la carte" manner and/or use compensating controls to create "enhanced" credentials. In several cases, **pilots enhanced broadly available social login credentials with additional factors.** For example, some pilots tied an event - such as a physical registration process - to the credential to strengthen it.

### *3.2.3. Coordinating Between Components*

A common challenge was the flow of user consent throughout identity architectures. Multiple pilots found it difficult to resolve the 'right level' of detail for consent interactions with the individual. While they sought transparency for informed consent, some felt that providing customers with too much information could be a burden and potentially cause user drop-off. **In response to this common problem, the pilots explored creative ways to manage consent and balance this tension.** For example, some pilots chose to share attribute types (e.g., name, address) in a consent dialogue with the user, while others chose to share actual data values (e.g., Jon Smith, 123 Constitution Avenue).

Pilots established a degree of interoperability through their use of open communication protocols. **Ultimately, open communications protocols are necessary but not sufficient to enable credential interoperability across multiple relying parties**. Such credential interoperability is more dependent on the multi-lateral acceptance of the processes supporting the credential issuance and the effect on business concerns – such as solution branding or the potential enablement of competitors by federating customer information – as well as the definition of the underlying credential data.

The different pilot architectures – as depicted in *Figure 1* above – illustrate how the binding operation between identity proofing and authentication varies in implementation. This has a profound effect on credential interoperability and reusability. For example, while the credential created in *Figure 1(b)* is interoperable in terms of reducing the number of credentials a user holds, the increased strength of the identity assertion that results from the RP's identity proofing may not be portable to other RPs. This provides some incremental benefit to credential reusability, but requires the individual to go through a second identity proofing event to achieve the same proofing strength at a second RP. Lastly, the scenario of *Figure 1(e)* facilitates the "enhancement" of credentials by an intermediary; however, the intermediary that created such credentials essentially "owns" them and must assume responsibility, providing ongoing lifecycle management.

### *3.2.4. Architecture and Components Conclusion*

Understanding the consequences of various identity architectures on the fulfillment of the GPs is a key step toward developing an accreditation scheme that aligns with the NSTIC. These varied architectures are especially evident when pilots separate identity proofing and authentication, or use intermediary components. Within the pilots, RPs recognized the importance of evaluating security and privacy characteristics of intermediaries in the Identity Ecosystem. As noted above, the boundaries between functions and participants are critical, as is the binding between the components. These architectural characteristics can impact adherence to all four of the GPs. There was also a tension between

pilots' desires to have identity architectures that were highly configurable and the need to have a defined and constrained system that could be readily assessed. This tension was particularly evident in componentized architectures where there were many different ways that the components could be combined and configured. All of these architectural factors need to be accommodated in a functional model that will serve as the basis for an assessment scheme. **Such a functional model would allow the clear identification of data flow and owners, so that identity systems can be effectively evaluated for their impact on the GPs of security, privacy, interoperability, and ease-of-use**.

## 3.3. Standards and Interoperability

The NSTIC called for interoperable identity solutions. However, without a suite of existing standards to guide their efforts, the pilots achieved limited interoperability; it was typically only supported in communication protocols. In order to develop interoperable identity solutions, pilots had to establish their own specific configurations of identity proofing, protocols to access APs, and binding mechanisms to create and provision digital credentials. This created a particular challenge in defining identity schema or data structures. **The pilots faced an absence of standards and a framework to support identity interoperability**.

Interoperability of pilot solutions would benefit from a common risk assessment process across multiple industries and COIs. Without a consistent way for multiple COIs to assess and communicate risk, there was limited ability to recognize the strength of a credential for use across multiple COIs. A related issue was that of evaluating and communicating the security of combined authentication technologies. If an organization used biometric authentication techniques along with a one-time password, it often found it difficult to evaluate the strength of this combined authentication method. In order to address these issues, pilots relied loosely on NIST SP 800-63-2 and OMB M-04-04 for mutual recognition and communication; however, these were just temporary fixes and should not be considered long-term solutions as these documents to do not sufficiently reflect the componentized state of the market.[27] **A standardized risk assessment, and a clear way to measure the strength of combined authentication technologies, would likely have eased the pilots' development of products that support interoperability, and the acceptance of these products in the market.**

The pilots' review of FICAM trust framework requirements highlighted a challenge when using smart phones to authenticate to federal systems. FICAM requirements are based on NIST SP 800-63-2, which specifies that modules performing cryptographic functions at certain levels of assurance shall be validated to Federal Information Processing Standards (FIPS) publication 140-2. **While cryptographic functionality on some smart phones has been certified under FIPS 140-2, the certification is only valid for specific versions of the operating system.** Thus, a smart phone's identity service application, when relying on cryptographic functionality, is only valid for approved versions of the operating system. This issue creates a significant barrier to consumer adoption – a key to the broader success of the Identity Ecosystem – since consumers generally upgrade their operating systems shortly after release. This issue also clearly impacts enterprises that have adopted a "bring your own device" policy, and therefore have limited control over the user's smart phone operating system version.

[27] *M-04-04: E-Authentication Guidance for Federal Agencies*, The White House, December 2003, https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

Pilots also faced challenges with commercial off the shelf (COTS) applications accepting third party credentials. In multiple pilots, the RP application was based on a COTS product. These products were licensed to the RP, and there were a variety of hosting configurations (on premises, managed service, etc.). This introduced an additional stakeholder in the establishment of the federated solution. Often the COTS products had native proprietary authentication solutions developed to support their specific product needs. **If an RP wanted the COTS solution to accept third-party credentials or attributes, it often required the COTS provider to modify the existing authentication functionality.** This type of fundamental change to the COTS product was often considered a strategic business decision and required the vendor's senior leadership buy-in to adjust the product roadmap.

The pilots encountered common challenges with knowledge-based authentication (KBA) for remote identity proofing, such as:

- There is a lack of guidance on how to configure KBA technology (e.g., types of questions that should be selected, number of questions, number of additional attempts allowed, number of diversionary questions allowed) to minimize the number of errors for the population of interest.
- Once the KBA solution had been configured, there was a lack of understanding of the expected error rates (i.e., false rejections, false acceptances, failures to enroll).

Due to these challenges, the pilots couldn't fully determine the effectiveness of KBA technology within their security solutions, or how well identity assertions based on it could be conveyed to other parties in their ecosystem.

To address these issues, **the pilots identified the need for a standard around KBA performance metrics for remote identity proofing**. The addition of standardized performance metrics to KBA would potentially allow organizations to more effectively make decisions regarding risk. To facilitate the development of this standard, the pilots collectively developed and submitted a draft proposal to the IDESG Standards Coordination Committee (SCC), suggesting the solicitation of a standards development organization to develop such a KBA standard.[28] The IDESG SCC is responding to this request.

In addition to shorter-term projects like cultivation of a KBA performance standard, the IDESG is focusing on longer-term efforts, such as developing an identity management requirements catalog for security, privacy, usability, and interoperability. The pilots have provided feedback on many of the proposed IDESG requirements, thus imparting their commercial experience onto the IDEF. This input will help to refine the requirements to be commercially viable, and,

[28] See *Appendix 5.4: Pilot Contributions to the IDESG*

perhaps more importantly, reflect **the governance policies and standards used across a broad range of COIs**. Without various frameworks able to recognize and accept credentials and processes being implemented by other trust frameworks, it is hard to imagine full realization of the NSTIC. This is a key challenge that the pilots are working to overcome, and the authors believe that the IDESG's accreditation scheme should target a degree of mutual recognition across trust frameworks.

# 4. Conclusion

In the two and a half years since the launch of the NSTIC Pilots Program, the pilots have enabled significant technological, business, and policy advances across the public and private sectors by identifying and addressing challenges in the Identity Ecosystem. In addition to accelerating the emergence of a commercial market, the pilots have helped to advance the infrastructure of the Identity Ecosystem via their own efforts and through the IDESG. Some of their interactions with the IDESG have been direct, such as contributing to the requirements in the first generation of the IDEF and the creation of the Periodic Table of Trust Elements. Others are indirect, through presentations of real world experience with federated identity systems, discussions, and the creation of definitions to be used widely in the identity space. No matter their specific role, all of the pilots have contributed to the expansion of the identity marketplace.

As the pilots' work continues, they are making an increasingly tangible impact. For example, pilots have ignited a growing number of private sector IdPs at different LoAs, as well as encouraging private sector RPs to shift from their proprietary authentication solutions to accepting third-party credentials. This provides individuals with the ability to choose different types of trusted digital credentials. Through these efforts, the number of individuals using federated identities – and the number of NSTIC-aligned identity transactions – is constantly growing.

While the pilots demonstrate a wide variety of architectures and approaches, the NSTIC Pilots Program has convened disparate organizations to work together in advancing NSTIC-aligned identity solutions. To that end, one consortium of firms that are normally rivals remarked that, "even if individual vendors in the identity space could develop a framework, it would be very difficult to get buy-in from other vendors who are competitors. With the recognition and funding from [the] NSTIC [NPO], the pilot activities gain the vendor neutrality, visibility, and credibility needed to get the various identity vendors to work together to develop a common framework that they can adopt."[29] This point, along with the observations articulated in this document, highlights why there is a great need for public fora in which common themes and market challenges around trusted identity can be addressed in a cooperative manner.

Pilots' experiences also helped to identify the need for a unifying framework for trust among Identity Ecosystem participants. They have made clear that this framework should also reflect commercially viable products, and offer material value to RPs and other members of the Identity Ecosystem. Pilots have also reinforced the need for a certification scheme based on this framework, to ensure that participants adhere to the NSTIC Guiding Principles.

[29] *Three Pilot Projects Receive Grants to Improve Online Security and Privacy*, NIST, September 2014, http://www.nist.gov/itl/nstic-091714.cfm

The path to create this framework requires all three focus areas of NSTIC implementation; the work of the IDESG, the pilots, and Connect.gov are all highly complementary efforts. As the implementation of the NSTIC advances, the NPO is placing greater emphasis on collaboration between participants across these three foci. With the Identity Ecosystem rapidly maturing, it is vital for the NPO to maintain a strong pilots program in the short-term that addresses the broad challenges to building the Identity Ecosystem.

Long-term, the Pilots Program, in conjunction with other identity management work at NIST, will have to shift its focus from addressing broad barriers to filling critical gaps in the Identity Ecosystem, continually evolving to help address market impediments as they emerge. Consistent with this long-term vision, the NPO recently released a solicitation specifically focused on advancing privacy-enhancing technologies, the first NPO effort to dedicate funding toward a single aspect of identity solutions. This follows a natural progression from the second goal of the NSTIC – to build and implement the Identity Ecosystem – to the fourth – ensuring the long-term success and viability of the Ecosystem.

As the Pilots Program evolves, the pilots' work will continue to be available as a resource to other organizations in the field, highlighting common themes, challenges, and successes. The NSTIC pilots will continue to inform the broader Ecosystem of their experiences and will assist the private sector in creating the Identity Ecosystem Framework. The pilots will also continue to catalyze development of the Identity Ecosystem by creating viable solutions and growing the marketplace for identity federation.

As stated by one pilot participant, "The pilot grant funding has helped us make the case to prospective partners. It allowed us to say that the U.S. government's lead on online identity [sees] this is a viable approach worth pursuing. This has had a significantly positive impact on our ability to grow our business." And, ultimately, a significantly positive impact on realizing the NSTIC vision of individuals and organizations utilizing secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.

# 5. Appendix

## 5.1. Acronyms

| | |
|---|---|
| AAAE | American Association of Airport Executives |
| AAMVA | The American Association of Motor Vehicle Administrators |
| ACT-IAC | American Council for Technology – Industry Advisory Council |
| AP | Attribute provider |
| AXN | Attribute Exchange Network |
| COI | Community of interest |
| COPPA | Children's Online Privacy Protection Act |
| COTS | Commercial off the shelf |
| CSDII | The Cross Sector Digital Identity Initiative |
| CSP | Credential Service Provider |
| DHS | Department of Homeland Security |
| DMV | Department of Motor Vehicles |
| FFO | Federal funding opportunity |
| FICAM | Federal Identity and Access Management |
| FIPS | Federal information processing standards |
| FNS | Food and Nutrition Services |
| FTC | Federal Trade Commission |
| GP | Guiding Principles |
| GSA | General Services Administration |
| GTRI | Georgia Tech Research Institute |
| IDESG | Identity Ecosystem Steering Group |
| IDEF | Identity Ecosystem Framework |
| IdP | Identity provider |
| ITL | Information Technology Laboratory |
| KBA | Knowledge-based authentication |
| LoA | Level of assurance |
| MFA | Multi-factor authentication |
| NCRIC | Northern California Regional Intelligence Center |
| NIEF | National Identity Exchange Federation |
| NIST | National Institute of Standards and Technology |
| NSTIC | National Strategy for Trusted Identities in Cyberspace |
| NPO | National Program Office |
| OIDC | OpenID Connect |
| OMB | Office of Management and Budget |
| PDS | Personal Data Store |
| PIV | Personal Identity Verification |
| PKI | Public key infrastructure |
| PRIVO | Privacy Vaults Online |
| RNS | Resilient Network Systems |
| RP | Relying party |

| | |
|---|---|
| SAML | Security Assertion Markup Language |
| SCC | Standards Coordination Committee |
| SP | Special Publication |
| TFP | Trust framework provider |
| TFS | Trust Framework Solutions |
| TSCP | Transglobal Secure Collaboration Participation, Inc. |
| UCAID | University Corporation for Advanced Internet |
| USAA | United Services Automobile Association |

## 5.2. Pilots: Learn More

More information about the NSTIC pilots can be found at:
http://www.nist.gov/nstic/pilots.html

To further explore the work of the NSTIC pilots, please visit their websites below or reach out to the contacts listed. In addition to their general websites, some recipients of NSTIC pilot funding have sites dedicated to their NSTIC pilot projects; these pages are listed below when available.

**2012 Recipients**

The American Association of Motor Vehicle Administrators (AAMVA)
Philippe Guiot, pguiot@aamva.org
http://www.aamva.org
http://www.aamva.org/Identification-Security/

Criterion Systems, Inc.
Dave Coxe, Dave.Coxe@Criterion-sys.com
http://www.criterion-sys.com
http://iddataweb.com/?page_id=67

Daon, Inc.
Cathy Tilton, Cathy.Tilton@daon.com
http://www.daon.com
http://www.trustx.com/

Resilient Network Systems, Inc.
Britton Wanick, brit@resilient-networks.com
http://www.resilient-networks.com
http://www.resilient-networks.com/nstic/

University Corporation for Advanced Internet Development (UCAID or Internet2)
Ken Klingenstein, kjk@internet2.edu
http://www.internet2.edu
https://spaces.internet2.edu/display/scalepriv/Scalable+Privacy

**2013 Recipients**

Georgia Tech Research Institute (GTRI)
John F. Wendelt, John.Wandelt@gtri.gatech.edu
http://gtri.gatech.edu
https://trustmark.gtri.gatech.edu/

ID.me, Inc.
Matt Thompson, matt@id.me
https://www.id.me
https://blog.id.me/welcome/

Privacy Vaults Online, Inc. (PRIVO)
Denise Tayloe, dtayloe@privo.com
https://privo.com
https://privo.com/nstic-grant-minor-trust-framwork/

Transglobal Secure Collaboration Participation, Inc. (TSCP)
Keith Ward, keith.ward@tscp.org
http://www.tscp.org
https://www.tscp.org/grants-1/nstic/

**2013 State Government Recipients**

Commonwealth of Pennsylvania
Frank Morrow, fmorrow@pa.gov
http://www.pa.gov/Pages/default.aspx

Michigan Department of Human Services
Cathy Fitch, FitchC@michigan.gov
http://www.michigan.gov/dhs

**2014 Recipients**

Confyrm
Andrew Nash, andrew@confyrm.com
http://www.confyrm.com

GSMA
Rafael Diaz, RDiaz@gsma.com
http://www.gsma.com

MorphoTrust USA
Patrick Clancey, pclancey@morphotrust.com
http://www.morphotrust.com
http://www.morphotrust.com/NSTIC

## 5.3. White Papers

**Daon**
H. Gunsinghe and E. Bertino, *Privacy Preserving Biometrics-Based and User Centric Authentication Protocol*, 2014, http://docs.lib.purdue.edu/ccpubs/635/

**ID.me**
Internet Retailer, *Under Armour Honors Heroes and Sees Affiliate Revenue Grow by Double Digits*, 2014, https://www.idecosystem.org/filedepot_download/1598/1317

**TSCP**
S. Russell, A. Slomovic, and P. Alterman, *Privacy in the Identity Management Landscape in the United States: Issues Raised by Using Employer-Issued Credentials for Personal Transactions*, 2014, https://www.tscp.org/wp-content/uploads/2014/10/Privacy-and-Employer-Credentials-White-Paper.pdf

**UCAID/Internet2**
Internet2, *Anonymous Credentials: A Report from the Internet2 NSTIC Pilot work in Scalable Privacy*, 2015, https://spaces.internet2.edu/download/attachments/86573103/Anonymous%20Credential%20WP%20012015.docx?version=1&modificationDate=1422550146115&api=v2

## 5.4. Pilot Contributions to the IDESG

### *5.4.1. Initial Contribution on KBA for Remote Proofing*

**Title:**
Performance metrics for knowledge based authentication (KBA) for remote identity proofing.

**Proposers:**
NSTIC pilots:
CSDII, Criterion, Daon, Resilient, UCAID
Exponent, GTRI, ID.me, PRIVO, TSCP
Commonwealth of Pennsylvania, State of Michigan
The NSTIC pilots were funded by the NIST NSTIC National Program Office (NPO). The NPO and its contractors supported the pilot collaboration meetings in which this work was developed.

**Submitted to:**
IDESG Standards Coordination Committee

**Submission date:**
March 26, 2014

**Description:**
Currently, there is a lack of standard performance metrics regarding the use of knowledge based authentication (KBA) for remote identity proofing. As a result, organizations that rely on these techniques for delivery of services to citizens and customers are forced to make critical authorization decisions with a limited understanding of the risks and benefits of the underlying technologies.
Identity and access management are essential aspects of information security to preserve the availability, confidentiality, and integrity of data, services, and resources. Like all other aspects of information security, selecting effective access control technologies, procedures, and policies requires mature risk management techniques; at the heart of which is an informed awareness of the inherent risks and benefits involved with a particular solution type. Currently, a lack of awareness regarding KBA and remote proofing requires that service providers, government agencies, and other organizations, assume risks that are not clear or well defined.

**Business case:**
The economic and organizational impacts of errors regarding access controls, whether involving KBA, remote proofing or other aspects of authentication and authorization, are all too clear in today's market. The results of data breaches—lawsuits, credit monitoring, and loss of sensitive data—can financially affect organizations, damage reputations, and or impact consumer confidence.

Conversely, well established standards around KBA and remote identity proofing will promote expanded and more effective risk-based processes and procedures, thereby increasing market confidence and driving adoption of these solutions. This increased adoption would then allow for a wider range of services to be moved on-line as in-person proofing processes are replaced by remote solutions. In addition, a clear statement of best practices will allow KBA vendors to articulate their solution differentiation.

**Existing practice and the need for a standard:**
In order to establish a more effective market that is responsive to the complicated requirements that service providers face today, standardized performance metrics and reporting procedures need to be developed. Once created, these standards would allow organizations, government agencies, and other service providers to effectively implement risk-based access solutions to meet cybersecurity needs, protect users, and ensure availability of services.
In order to help establish a common understanding of KBA and remote identity proofing services, it is proposed that standardized approaches are developed to:

1) determine the accuracy and efficacy of KBA and remote proofing techniques. This may include requirements for the currency and validity of the information used in the proofing or the development of the KBA questions; and
2) report failure rates of KBA systems. In addition to standardizing validity criteria for data and processes used in the proofing process or KBA question development, this standard will establish reporting requirements for false acceptance, false rejections, and failure to enroll.

**Impact on existing or potential markets:**
This standard would have a positive impact on the existing identity and access management market by providing a common understanding of KBA and remote proofing standards, improving confidence in solutions, and improving risk-based decision making. Additionally, this standard would improve access to services across multiple markets (health care, financial services, online services that fall under the FTC Children's Online Privacy Protection Act, etc.) that require identity proofing to provide services that require high assurance identity solutions.

**Existing standards and related work**
No existing standards relating to performance metrics for Knowledge Based Authentication for remote proofing of identity have been identified. The closest related work discovered is a report by the IDPV Identity Resolution Project on "Establishment of Core Identity Attributes Sets and Supplemental Identity Attributes" (Document No. NASPO-IDPV-060) which analyzed a large database of identity attributes to determine sets of attributes that could be used to resolve individuals from that database. Thus, the NASPO paper's principle purpose was to determine attribute sets for identity resolution, rather than to consider attribute verification for identity proofing. However, to the extent that certain attributes that may be used for KBA were not available within an attribute set (creating what

was classified as a “null identity” in the paper), the paper may inform a standard that is developed based on this proposal by identifying one reason for failure in a KBA system.

*5.4.2. Additional (Requested) Contribution on KBA for Remote Proofing*

## From
NSTIC Pilot Collaboration Group

**To**
IDESG Standards Coordination Committee

**Date**
March 20th 2015

**Background**
On March 27, 2014 the NSTIC pilot collaboration group forwarded a proposal regarding *Performance metrics for knowledge based authentication (KBA) for remote proofing* to the IDESG Standards Coordination Committee (SCC). We understand that the SCC conducted a call for standards organizations to solicit their interest in developing a standard based on the proposal, but they have not yet identified an organization that meets the IDESG SCC selection criteria.

As a consequence, last month the SCC asked the pilot collaboration group to provide supporting material for the proposal that could be forwarded to appropriate organizations. It is our understanding that the NASPO IDPV committee that was identified in the proposal is a possible target organization for this additional material. We suggest that an additional body for consideration would be the Accredited Standards Committee X9 (ASC X9). As you likely know, ASC X9 has a history of developing identity related standards for financial transactions, such as ANSI X9.84 *Biometric Information Management and Security for Financial Services Industry* and ANSI X9.117 *Secure Remote Access Mutual Authentication*. Due to the financial sector's historical use of KBA, X9 committee members may be sufficiently motivated and knowledgeable to develop the standard proposed by the NSTIC pilots.

This response to the SCC request comprises the observations from several of the NSTIC pilots. The overall pilot collaboration group has reviewed this response. The pilot collaboration group would be pleased if the IDESG SCC would forward this response directly to the standards organizations that the SCC deems appropriate.

In this document, we use the term *integrator* as the organization that is relying on the KBA technology, the term *user* to denote the individual who is using the integrator's application, and the term *vendor* to denote the provider of the KBA technology.

**Pilot response**

**Overview**
KBA technologies tend to operate on a two-step process.

KBA step 1. The application user provides a minimal set of user information which is used by the KBA vendor to determine the uniqueness of the presented data set, and the availability of associated historical data to generate the KBA questions.

KBA step 2. The KBA questions are posed to the user and, based on their responses, the KBA vendor provides a YES/NO answer to the integrator, to indicate whether the user is the valid holder of the data set of user information presented in step 1.

In general, the comments from the pilots fall into two categories:

Integrators need to know that they are doing the best that they can with the KBA technology, based on the population of interest, and;
Integrators need to know what residual risk they are assuming based on system performance.

Thus, the pilots requested guidance on setting up and using the KBA technology, as well as the standardized reporting of specific performance metrics that would help them understand their residual risk.

**Suggested Guidance**
General

KBA technologies for remote identity proofing tend to be configurable. It would therefore be desirable to have standardized guidance for the configuration of the vendor technology by the integrator. This could be accomplished by the integrator selecting from a standardized series of population sets, based on characteristics such as expected range of credit history, expected address stability, etc. The selected population set would then establish the configuration required by the vendor.

In regards to KBA step 1

It is would be helpful to know the expected performance of the KBA system as a function of the provided user data set. This would allow the integrator to invoke KBA at the correct stage in their process. Too early and there are not enough data to meaningfully resolve individuals; too late and more than the necessary amount of data has been requested of the user.
Based on the minimal sets of data, what is the expected accuracy, and what is the expected ratio of real to diversionary questions that will be used in step 2?

In regards to step 2

- It would be helpful to have a standardized way of displaying questions across vendors and devices.
- What questions are asked when there is minimal financial or address history?

**Reported performance metrics:**

Based on the population set selected by the integrator:

- What is the percentage of that population set for which sufficient identity resolution data is unavailable and who would fail KBA step 1 above?
- For the population for which there is sufficient identity resolution and KBA data, what is the expected false rejection rate (i.e. legitimate users who fail the KBA step 2)?
- For the population for which there is sufficient identity and KBA data, what is the expected false acceptance rate (i.e. users who are misclassified as different legitimate users in KBA step 2)? This metric would indicate the degree of confidence or assurance to the integrator to allow them to manage their risk appropriately.

These performance metrics should be reported along with a statement of the database characteristics used to generate the expected values for the population set.

### *5.4.3. Pilot Contribution to the IDESG on Interoperability Requirements*

**Overview of Pilot Feedback: Interoperability Requirements**
*September 12, 2014*

The pilots reviewed the interoperability derived requirements. They identified the following three considerations vital to the success of each requirement:

- **Is it commercially viable today?** Some of the drafted interoperability requirements are not feasible in the current market, and thus would be better suited as guidelines. The wording could reflect this by stating that organizations "should" follow a requirement as opposed to "shall".
- **Is it specific to particular actors in the ecosystem?** Many of the draft interoperability requirements are not equally applicable to all roles. Narrow requirements should be clearly targeted to a particular actor, or they should be broad enough to apply to all.
- **To which LoAs does it pertain?** Interoperability requirements must specify the level of assurance that is associated with each specific requirement, since interoperability concerns will vary between lower and higher LoAs.

The pilots provided specific feedback to the IDESG on three distinct interoperability requirements:

- **Requirement 28: "**Organizations shall utilize technologies that communicate and exchange data based upon well-defined and testable interface standards."
    - **Discussion:**
        - Is this SAML/OpenID Connect? Or could it use ex. Facebook? Is someone precluded from offering others in addition to SAML, etc.? This seems focused on the CSPs, not the RPs.
    - **Feedback for IDESG:**
        - We recommend SAML and OpenID Connect for all assurance levels, and others for lower levels to be supported by IdPs. A similar standardized protocol should be created for APs but this is aspirational at this point. Aspirationally, RPs should also be included, but at this time market forces make this challenging.
- **Requirement 27: "**Organizations shall issue credentials capable of being utilized by multiple different service providers."
    - **Feedback for IDESG:** IdPs shall issue credentials capable of being utilized by multiple different RPs (we are assuming Service Providers = RPs). Need to consider more policy around level of assurance, in terms of what utilized means.
- **Requirement 31: "**Organizations shall utilize solutions and technology that allow for identity portability."

- **Feedback for IDESG:** There is no current format for this and perhaps this requirement may be more focused on the portability of metadata regarding consent, etc. Work is developing in this area but it should not be a near term requirement.

Overall, the pilots support the creation of interoperability requirements and believe that additional requirements, potentially for attributes and relying parties, will be needed in the future. Effective baseline interoperability requirements, combined with advances in the marketplace, are imperative to enhance interoperability between all actors in the identity ecosystem.

*5.4.4. Pilot Contribution to the IDESG on Privacy Requirements*

**NSTIC Pilots' Feedback: Privacy Requirements**
*November 4, 2014*

**Overview:**
Over the course of several working sessions, the NSTIC pilot participants reviewed the requirements on the IDESG wiki, developed by the IDESG Privacy Committee as of 9/30/14. The pilots offer the following feedback on the requirements, organized as: general comments; and specific comments on the requirements, with suggestions for change or for discussion.

The pilots recognized that the IDESG Privacy Committee is navigating relatively unchartered territory since there is a lack of privacy standards today. While the pilots suggest that the requirements require further consideration and adjustment, it is believed that the requirements present a promising start, and that they will play a vital role in establishing a privacy-enhancing identity ecosystem.

The following NSTIC pilots participated in some or all of the pilot collaboration meetings on this topic:

CSDII, Criterion, Daon, UCAID
GTRI, ID.me, PRIVO, TSCP
Commonwealth of Pennsylvania, State of Michigan

The NSTIC NPO and its contractors supported the pilot collaboration meetings in which this work was developed.

**Submitted to:**
IDESG Privacy Committee

**Submission date:**
November 14, 2014

**General Comments:**

- **The requirements should be at a similar level.** Some of the requirements are for specific parts of a transaction while others are very high level and do not include any privacy specific language.
- **Is the goal to have attestable requirements?** If the goal is to attest (or be verified) against these requirements, then they need to be broken down further and explained with more specifics. In addition to specifics, examples of mechanisms or solutions could be included to help organizations better understand how to apply and comply with the requirements
- **Emphasize the relationship versus the transaction.** In many of these requirements a specific transaction is mentioned, but often the

relationship between a relying party and a user goes beyond one transaction. The requirements must consider the longer term relationship in addition to individual transactions.

- **Consider the relationship between identification and the level of service provided.** Several requirements discuss the degree of identifying information being provided be proportional to the risk of the transaction. It may be beneficial to also consider the degree of identifying information provided be proportional to the benefit provided by a service provider.
- **The risk being discussed seems to be focused on the RP:** There are many types of privacy risk and the risk discussed in the requirements should include risks to the user, IDPs, and others, just not RPs.

**Specific Comments on the Requirements:**

- **Requirement 1: "**Organizations shall limit the collection and transmission of information to the minimum necessary to fulfill the transaction's purpose and related legal requirements."
    - **Suggested Change:**
        - Replace "transaction" with "relationship"
    - **Questions and Areas for Discussion:**
        - Need to consider the concept of proportionality. The amount and sensitivity of information collected and transmitted should be proportional to the risk of, and/or benefit provided by, the transaction.
        - The relationship could include multiple sessions and there may be multiple transactions in one session
- **Requirement 2: "**Organizations shall limit the use of the individual's data that is collected and transmitted to the specified purposes of the transaction."
    - **Questions and Areas for Discussion:**
        - Specifics are needed around how the information could be used.
        - This information is usually explained in the terms of service, ULA, or privacy policy: is this not sufficient?
- **Requirement 3: "**Organizations shall limit the retention of data to the time necessary for providing and administering the services and transactions to the individual end-user for which the data was collected, except as otherwise required by law."
    - **Questions and Areas for Discussion:**
        - More specificity is required here especially around time necessary.
        - The history of user activities should also be included in this, not just data.
        - What is the intent of this requirement: to require disclosure of retention policies to the user?

- **Requirement 4: "**Organizations shall provide concise, meaningful, timely, and easy-to-understand mechanisms to communicate to end-users how they collect, use, disseminate, and maintain personal information."
    - **Questions and Areas for Discussion:**
        - Are there standard definitions for "concise, meaningful, timely, and easy to understand"?
        - How do the mechanisms align with sector specific best practices?
        - Examples and tools are needed to explain "mechanisms" to support these requirements
        - This could be a challenge for self-attestation as it could be difficult for organizations to legally represent this
- **Requirement 5: "**Organizations shall minimize data aggregation, including linkages across transactions."
    - **Suggested Change:**
        - "Data aggregation" should be changed to "PII aggregation".
        - "linkages" to "account linkages"
    - **Questions and Areas for Discussion:**
        - What is the desired outcome of this requirement?
        - Seems to be at a higher level than some of the requirements
        - Adding specificity to this requirement would help with attestation
        - As this currently reads, the need to maintain audit trails would make compliance unlikely or at least complicated
- **Requirement 6: "**Organizations shall provide appropriate mechanisms to enable individuals to access, correct, and delete personal information."
    - **Questions and Areas for Discussion:**
        - Pilots often are verifying data against (at least notionally) authoritative sources. "Mechanisms" may be with second level support to allow the individual to contact the authoritative sources directly, much as financial institutions provide credit bureau contact information for redress and issue resolution.
        - Does delete include the right to be forgotten?
- **Requirement 7: "**Organizations shall determine the necessary quality of data used in identity assurance solutions based on the risk of that transaction, including to the individuals involved."
    - **Questions and Areas for Discussion:**
        - A data quality standard needs to be developed by an SDO or similar organization to support interoperable and consistent application of this requirement.
        - What is meant by "data quality" Is the requirement about the least amount of information needed to get the appropriate level of data quality?

        - This is the first time privacy has been linked with the risk of a transaction
        - This seems to be more of a security committee requirement
- **Requirement 8: "**When terminating business operations or overall participation in the Identity Ecosystem, organizations shall, while maintaining the security of individuals' information, transfer it upon their request and destroy it unless they request otherwise."
    - **Questions and Areas for Discussion:**
        - There should be an obligation to notify the user when their data is either destroyed or transferred with some notice before an action is taken
        - If the company is out of business how would this be enforced?
        - Is there a standard format for this transfer?
        - Are there requirements around where it can be transferred?
- **Requirement 9: "**Organizations shall be accountable for conformance to these requirements, and provide mechanisms for auditing, validation, and verification."
    - **Suggested Change:**
        - This should be deleted
    - **Questions and Areas for Discussion:**
        - This seems like it is a higher level requirement relating to participation in the IDESG ecosystem certification program
- **Requirement 10: "**Organizations shall provide effective redress mechanisms for, and advocacy on behalf of, individuals who believe their rights under these requirements have been violated."
    - **Suggested Change:**
        - Delete "and advocacy on behalf of"
    - **Questions and Areas for Discussion:**
        - Advocacy is out of scope.
        - Provide examples of appropriate redress mechanisms.
        - "Effective" should be defined
- **Requirement 11: "**Where individuals make choices regarding the treatment of their information (such as to restrict particular uses), those choices shall be automatically applied to all parties downstream from the initial transaction."
    - **Questions and Areas for Discussion:**
        - This may not be possible with current technology
        - How can this be achieved without tracking and linking ?
        - Does this require a standard be created for user preference metadata?
        - Who are the "parties downstream" that the requirement is mentioning?
        - Is the enforcement limited to contracts?  Does there need to be a technical solution today?

- **Requirement 12: "**Organizations shall, where feasible, utilize identity solutions that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, and/or uniquely identified."
    - **Suggested Change:**
        - Remove "where feasible"
        - "Organizations" should be changed to RPs, if this relates only to the consumption of such services. It is not clear that all identity services would be required to provide a full range of options, but it seems clear that organizations that rely upon the identity services should support all options.
        - Prioritize "anonymous" first and "uniquely identified" last, to create a spectrum of solutions ranging from zero- to minimal- to full-identification.
    - **Questions and Areas for Discussion:**
        - Is the goal of this for the organization to follow the concept of proportionality and use the minimum information needed for the transaction?
        - This requirement needs a definition of uniquely identified if it is going to be included in this list.
        - In an attestation, organizations may just check the box due to the "where feasible" language
- **Requirement 13: "**Organizations will request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction."
    - **Suggested Change:**
        - **"**Organizations will only request from the individual the minimally-identifying identifier required according to the risk of the transaction"
    - **Questions and Areas for Discussion:**
        - Please clarify "when necessary" as it makes attestation difficult.
        - Is "request credentials" the correct terminology? It may not be understood by many members in the ecosystem
- **Requirement 14: "**Participation in the Identity Ecosystem shall be voluntary."
    - **Suggested Change:**
        - This seems to be out of scope
- **Requirement 15: "**Privacy controls should be situated as low in the technology stack as possible."
    - **Suggested Change:**
        - "privacy controls should be situated in the technology stack"
    - **Questions and Areas for Discussion:**
        - This is more of a principle than a requirement as it cannot be measured or enforced

        - Is this suggesting technical controls are preferred to a policy solution?
        - Why is lower in the technology stack better and who will determine what is low enough?
- **Requirement 16: "**Organizations shall clearly indicate to individuals what personal information is mandatory and what information is optional prior to the transaction."
    - **Suggested Change:**
        - "prior to sharing" or "prior to collection" instead of "prior to transaction"
    - **Questions and Areas for Discussion:**
        - The committee should consider clarifying what is meant by "indicate". This could be separated into "notification" and "consent" but it is unclear which this requirement is intended to address
        - Where is the line between mandatory and optional information and who is going to enforce that line?
        - What does prior to the transaction mean? Before authentication, before collection?
- **Requirement 17: "**Controls on the processing or use of individuals' information shall be commensurate with the degree of risk of the processing or use."
    - **Suggested Change:**
        - Consolidate this with other risk based requirements
    - **Questions and Areas for Discussion:**
        - This seems more of a general principle than a requirement. What type of controls (i.e. technical or policy) are being referred to in this requirement?
        - Is "information" focused on identity information, attributes, other?
- **Requirement 18: "**Identifiers shall be segregated from attributes whenever feasible."
    - **Questions and Areas for Discussion:**
        - It is unclear what the purpose of this requirement is, particularly considering attribute, identifiers, and tokens are all attended to be bound in order to support use in transactions
        - "wherever feasible" limits the value of the requirements.
        - Is this requirement referring to data storage and what is meant by segregated
        - Identifiers are a type of attribute so this seems impossible

*5.4.5. Pilot Contribution to the IDESG on Security Requirements*

**NSTIC Pilots' Feedback: Security Requirements**
February, 19, 2015

**Overview:**
Over the course of several working sessions, the NSTIC pilot participants have reviewed the initial set of IDESG Security Requirements. The pilots offer the following feedback on the requirements, which include both general comments on the overall set and specific comments on individual requirements. Where identified, suggestions for change or for discussion have also been included.

The pilots recognize that substantial work that has been done on these requirements to date. While there are suggestions for further consideration and adjustment, it is believed that the requirements represent a well thought-out and nearly complete set of requirements that, once refined, will support a secure and resilient Identity Ecosystem.

The following NSTIC pilots participated in some or all of the pilot collaboration meetings on this topic (not all of the feedback presented here was unanimous, but it does represent the consensus views expressed at the meetings):
Daon, GTRI, ID.me, PRIVO, Criterion, TSCP, UCAID, Morphotrust, Confyrm, GSMA, State of Michigan, Commonwealth of Pennsylvania.

The NSTIC NPO and its contractors supported the pilot collaboration meetings in which this work was developed.

**Submitted to:**
IDESG Security Committee

**Submission date:**
February, 19, 2015

**General Comments:**
- **Consistent Terminology.** "User" and "end-user" are utilized interchangeably throughout the full set of requirements. The Security Committee should remember that for some services, the user may actually be the organization that purchased the solution. The committee should seek to clarify in all cases who the "user" is (e.g., individual consumer or organization relying on the solution).
- **Flexibility v. Levels of Assurance.** Most of the pilots appreciated the flexibility afforded by the "outcome based" requirement statements and the inclusion of language such as "commensurate with risk," but questioned how requirements with this language would align with the definition of a baseline set of requirements. Is it intended that the baseline set of requirements addresses the steps that shall be taken in a low risk

scenario, and that additional security steps may be taken in higher risk scenarios? This was a more general statement addressing the full state of IDESG requirements, not specifically the Security Requirements.

- **Requirements should be mapped to individual functions rather than core operations.** Currently the Security Requirements are mapped to the functional model's core operations. However, several of the pilots expressed the desire to see them mapped to the individual functions since their services may only play a small part in one or several core operations. They felt the more granular breakdown allowed for clearer and more accurate understanding of which requirements applied to their solution.
- **Functional Model Roles.** The inclusion of roles in the functional model, with associated functions and core operations, confused several pilots as to how they should appropriately describe their service. The language prefacing the section on roles should be even more explicit in pointing out that the defined roles are merely illustrative of the types of functions commonly executed by such roles, but are not intended to restrict services. The committee should discuss whether to remove this description going forward or make it clearer.
- **Testability.** While it is clear that these are the first set of requirements designed for self-assessment there are concerns about how conformance to the requirements would ultimately be tested. Language such as appropriate, proper, industry best practices, and operational risk will be very challenging for third party assessment and may even cause confusion with self-assessment. Consistency of requirements language throughout the process from self-attestation to (possible) third-party testing will allow product developers to more clearly formulate their product roadmaps.

**Specific Comments on the Requirements:**

- **Include new requirements that address the following:**
  - **Notification of a compromised credential. Should address who should be notified, including the individual owner of the credential.**
  - **Revocation of credentials and tokens.**
- **Requirement 1:** Service providers in the ecosystem follow recognized information security standards, frameworks, and/or appropriate practices.
  - **Suggested Change:**
    - None
  - **Questions and Areas for Discussion:**
    - Will need to clarify that the standards and frameworks in the spreadsheet are informative references and conformance is not required of participants. A larger list of standards and full mapping would also be very useful to participants.

        - Is this requirement also covering implementation of the standards or frameworks? Is the applicant attesting that they have implemented it correctly?
- **Requirement 2:** Each account credential pair is uniquely identifiable for authentication purposes.
    - **Suggested Change:**
        - Modify the last line of the supplemental guidance: “should not be used to enable tracking of users or to limit the application of pseudonymous/anonymous transactions except where consent has been provided by the user or delegate."
    - **Questions and Areas for Discussion:**
        - Some cases will exist where users (or designated delegate such as a parent) want to allow services to track their behavior or activities. The supplemental guidance should not restrict this, so long as consent has been provided.
        - Committee should be aware that this may need to take place at several locations in the ecosystem—for example at both the RP and the CSP.
- **Requirement 3:** The confidentiality and integrity of identity data (e.g., attribute values) is protected during the execution of all identity functions and across the entirety of the data lifecycle (collection through destruction).
    - **Suggested Change**:
        - Add to the supplemental guidance language stating that data is encrypted as soon as possible and that it spends minimum possible time unencrypted.
        - State the “integrity” refers to the security objective, not the accuracy of the data.
        - Add insider threat to the list of threats in the supplemental guidance.
    - **Questions and Areas for Discussion:**
        - In some cases identity related processes will necessarily take place in unencrypted space. So long as the collected data is encrypted as soon and as long as possible then it should fulfill this requirement.
- **Requirement 4:** Credential and token issuance processes protect against unauthorized disclosure and/or reproduction.
    - **Suggested Change**
        - None
    - **Questions and Areas for Discussion:**
        - Add notification requirement for discovery of a compromised credential or token?
- **Requirement 5:** Users are able to authenticate the source of all token and credential data received from service providers.
    - **Suggested Change:**

        - Change “authenticate” to “verify.”
        - Provide additional supplemental guidance clarifying the degree of verification intended by this requirement statement. Perhaps include examples.
    - **Questions and Areas for Discussion:**
        - Is this simply TLS with properly implemented certificate for the service provider’s website? Is it digitally signed software updates? Does this require encrypted and digitally signed emails for account notifications? Is it a combination of these? The answers to these will determine if this is realistically able to be implemented by service providers.
        - Could this be addressed through the explicit inclusion of TLS in the supplemental guidance for requirement 3?
- **Requirement 6:** Credentials and associated tokens are granted to the appropriate and intended user(s) only.
    - **Suggested Change**:
        - In supplemental guidance, add statement that “appropriate user(s)” could be a designated or legal representative (i.e., parent for a minor).
    - **Questions and Areas for Discussion:**
        - In consumer facing and enterprise use cases there may be situations where a credential is granted to a designated representative on behalf of an individual or group. While this would likely fall under “appropriate user(s)” several pilots felt it was worth mentioning in the supplemental guidance.
- **Requirement 7:** There are clear processes, policies, and procedures in place for the execution of identity functions.
    - **Suggested Change**
        - Reword to: There are clear, documented processes, policies, and procedures in place for the execution of identity functions.
        - In supplemental guidance change “management of operational risk” to “management and mitigation of operational risk.”
    - **Questions and Areas for Discussion:**
        - In the supplemental guidance it mentions the management of operational risk but does not mention using controls to mitigate the risk. Also is this guidance proposing that operational risk is a subset of, or is caused by, the identity function?
        - The two sentences in the supplemental guidance seem unrelated.
- **Requirement 8:** End users have access to the policies and procedures in place for the execution of identity functions.
    - Suggested changes
        - End users have access to relevant procedures…

    - **Questions and Areas for Discussion:**
        - Individual users should not have carte blanche access to any and all security policies that may be in place at service providers. Service providers should provide notice of relevant policies related to security and privacy.
        - This may be more consistent with a usability requirement. It seems to be intended to address a degree of transparency with respect to how services operate rather than the security of the service.
- **Requirement 9:** The confidentiality and integrity of authentication data are protected. Data (such as passwords and passphrases) used for authentication are never stored in plaintext.
    - **Suggested Change:**
        - Combine with requirement three. Address the issue of password storage in the supplemental guidance.
    - **Questions and Areas for Discussion:**
        - The confidentiality of authentication data may only be ensured by service providers once matched. The matching process sometimes takes place in an unencrypted space, for example with biometric systems.
        - The committee may want to consider that some legacy systems will require plaintext versions of passwords. They can still be protected through other measures besides encrypting, hashing, and/or salting. Perhaps the supplemental guidance could state, “it is highly recommended that passwords are never stored in plain text.” Specific measures for protecting plaintext passwords could be added to augment this language.
        - The final sentence in the guidance is confusing. Hashing is not encryption and it almost suggests that encryption can be skipped. Update the guidance so that it is clearer as to whether the intent is for hashing to replace encryption or whether is intended to augment encryption. This suggests I could store passwords in an unencrypted database so long as the values are hashed—is that the intent? Remove the reference to hashing as “one way encryption.”
- **Requirement 10:** User control of the token is proven during the authentication process.
    - **Suggested Change:**
        - Provide clarifying language on “control.”
    - **Questions and Areas for Discussion:**
        - At least one participant was unclear what was meant by “control” of the token and how it may differ from “possession.” Requested that clarifying language be added to the supplemental guidance.

        - Suggest reviewing 800-63 distinction between “control” and “possession”—control requires a physical token to be present during authentication, which would make a second factor or the use of physical tokens required within this scheme.
- **Requirement 11:** Users must be able to choose authentication mechanisms that are stronger than single factor passwords and passphrases and are commensurate with the level of risk associated with the transaction.
    - **Suggested Change:**
        - No specific change, but additional language is needed to relay the intent of this requirement.
    - **Questions and Areas for Discussion:**
        - Committee should consider that service providers may offer stronger authentication options which are not implemented by relying parties. How would this impact a CSP’s self-certification—would it be by implementation? Or, for the overall service and the options it provides?
        - Is the intent of this language to require second factor authentication options? The language of the requirement suggests that single factors could still be used so long as they are “stronger” than single factor passwords. This concept of “stronger” is going to be very difficult to enforce since it implies comparative determinations which—in most cases—do not exist. A service provider could state that their solution is stronger than a password, but there is unlikely to be objective statistics to quantify this position.
- **Requirement 12:** Service Providers have established policies, procedures, and processes in place to maintain availability of services.
    - **Suggested Change:**
        - None
    - **Questions and Areas for Discussion:**
        - None
- **Requirement 13:** Where cryptographic solutions are used, key management policies and practices are established and used consistent with industry standards and best practices.
    - **Suggested Change:**
        - None
    - **Questions and Areas for Discussion:**
        - Include more standards for reference
        - While FIPS 140 is not a key management standard, the committee should be aware that it may be referenced by others with respect to this requirement. There are some concerns with FIPS 140 and its capability to support solutions based on mobile solutions.

- **Requirement 14:** Processes for the reissuance and/or recovery of credentials and authentication tokens are commensurate with the original process and procedures followed during registration and credentialing core operations, including identity assurance procedures.
    - **Suggested Change:**
        - Current language suggests that “reproofing” would need to occur in order to complete this requirement. Suggest rewording to: ‘Processes for the reissuance and/or recovery of credentials and authentication tokens preserve the security and assurance of the original registration and credentialing operations.
    - **Questions and Areas for Discussion:**
        - Most pilots stated they had implemented recovery processes that incorporate out-of-band techniques and additional verification, but did not include full “reproofing” or a full reissuance and re-registration process. Most agreed this would be an unrealistic requirement.
- **Requirement 15:** Transactions and security events (to include the execution of identity functions) are logged in a manner that supports system audits and, where necessary, security investigations. Timestamp synchronization and granularity are appropriate to the level of risk associated with the environment, sector, or transaction.
    - **Suggested Change:**
        - For second sentence, add “internal system” to beginning.
        - Need to include language about logging supporting organizational and regulatory requirements in addition to audits and investigations.
    - **Questions and Areas for Discussion:**
        - Just clarify that there is no requirement to synchronize with an external clock (e.g., NIST nuclear clock).