We identify our friends and loved ones
by the look of their face,
over the phone by the sound of their voice
and in the dark by the touch of their hand.

Imagine being able to quickly identify someone on the internet with the same level of certitude.

Daon

NSTIC

Daon TrustX Pilot

P. Godwin

30 January 2014

kantara INITIATIVE™

Work described in this presentation was supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office and the National Institute of Standards and Technology (NIST).

The views in this presentation do not necessarily reflect the official policies of the NIST or NSTIC, nor does mention by trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Daon Background

- Daon is best known for our large scale biometric identity assurance systems:
  - National ID systems – Mexico, India, Portugal, Qatar
  - Border management systems – EU, Japan, Australia, NZ, US
  - Biometric enrollment and background screening services
- Primarily “In-Person” identity authentication
- Daon “guiding principles” and differentiators
  - Device, technology and vendor neutral
  - Open, standards-based platform approach
  - Built into the core technology all of the “ilities” – scalability, adaptability, flexibility, availability, reliability,

Homeland Security

Evolution to "remote identity authentication"

- Following the explosion in growth of Smartphones Daon decided to apply its core technology and guiding principles to the problem of "remote identity authentication" (e.g. on-line authentication)
- From this, IdentityX, Inc. was born

On-Going Pilots with some of the worlds largest banks

IdentityX Mobile Authentication Solution Named in Leading Analyst Firm's Annual "Cool Vendors" Security Solutions Report

Vendors selected for the "Cool Vendor" report are innovative, impactful and intriguing

RESTON, Va., X June, 2012 – IdentityX®, an av
authentication solution, was profiled by Ant
recently released *Cool Vendors in Security: Id
Management, 2012** report. According to th
report, the six companies covered provide h
enhanced technologies within the identity a
(IAM) market.

Daon

Terman 2011 WINNER

IdentityX™ Wins Cyber Security Category at American Technology Awards

Innovative security platform honored by TechAmerica Foundation

Reston, Va. – Daon has been named the winner in the Cyber Security & Authentication category for the American Technology Awards, which bestows the only "Best Of" awards that recognize all technology products and services for the technology industry. The award was attributed to IdentityX, the mobile authentication solution that significantly decreases the risk of unauthorized transactions, protecting businesses and consumers against on-line fraud and hacking.

TrustX and NSTIC

- Daon begin considering the possibility of providing its IdentityX capabilities as a cloud-based service offering to a range of Relying Parties. At the time we dubbed this service as a “Digital Identity Authority” (DIA)
- Established TrustX Technologies, Inc. (a subsidiary of IdentityX) as the incubator for the DIA concept
- Announcement of NSTIC Grants Competition
- Daon 1-of-5 first round awardees

Proprietary and Confidential

Daon Key Objectives for our NSTIC Involvement

- Create a full-service IDP (TrustX IDP) that:
  - Is based on IdentityX authentication technology
  - Conforms to Daon guiding principles
  - Aligns to NSTIC guiding principles
  - Supports multiple authentication protocols and trust frameworks
  - Is assessed and approved compliant with various authorities:
    - Kantara Initiative
    - SAFE-BioPharma
    - FICAM
- Market this capability to government and commercial customers nationwide:
  - Make TrustX IDP accessible via FCCX
  - Make TrustX IDP accessible via Criterion AXN
  - Make TrustX IDP the “strong authentication” platform for other IDPs such as ID.me
  - Market directly to a variety of RPs

Proprietary and Confidential

Our Team

Daon

Advancing Commercial Participation in the NSTIC Ecosystem

AARP®

BANK Major Bank

PayPal

PURDUE UNIVERSITY

AAAE AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

What are we investigating?

- Suitability of strong, mobile-based authentication technology (including biometrics) for online authentication
- Willingness of RPs to move to external identity/credential providers and how this fits within their business models
- Acceptance of subscribers
- Capability of existing trust frameworks (& certification schemes) to support these scenarios & technology
- Degree of interoperability achievable

Proprietary and Confidential

Our Pilot Elements

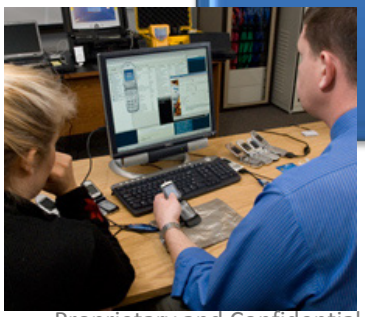
Daon

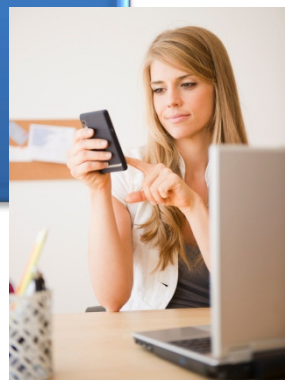
Technology

Trust Frameworks

Research

Operational Pilots



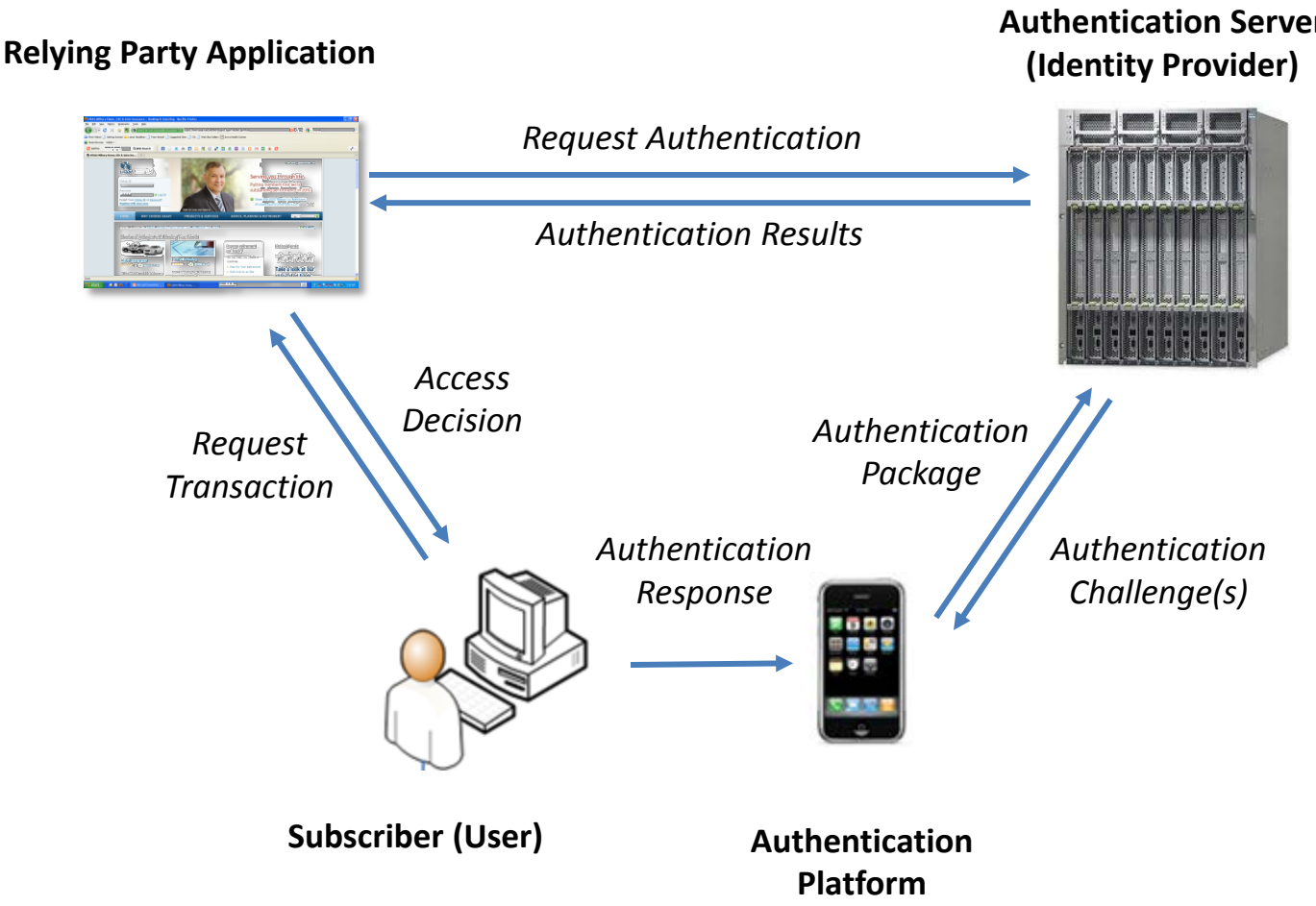


Core Technology: IdentityX

- A unique risk-based, multi-factor authentication capability that leverages latest generation smart phones (e.g., iPhone, Android, Windows Phone, Blackberry,), smart tablets (e.g., iPad/Playbook) and traditional mobile devices
- IdentityX technology combines multiple authentication techniques for greatest identity confidence:
  - Device (What you have)
  - PKI Certificate (What you have)
  - PIN/PW (What you know)
  - Face (Who you are)
  - Voice (Who you are)
  - Palm (Who you are)
  - GPS (Where you are/context)
  - OOB OTP (What you have)
  - (other as devices enabled)
- Placing biometric levels of identity assurance in the hands of consumers
- Designed to run both as an in-app framework and out-of-band authentication product

Technology - IdentityX

Daon



IdentityX®

Video Introduction to IdentityX

http://www.youtube.com/watch?v=Du08ccwaVEg

TrustX IDP

- Based on IdentityX authentication we have:
  - Created an platform and service offering for delivering highly secure authentication services to businesses and consumers
  - A multi-tenant service hosting multiple applications from different Relying Parties
  - Operating within multiple trust frameworks

TrustX Services

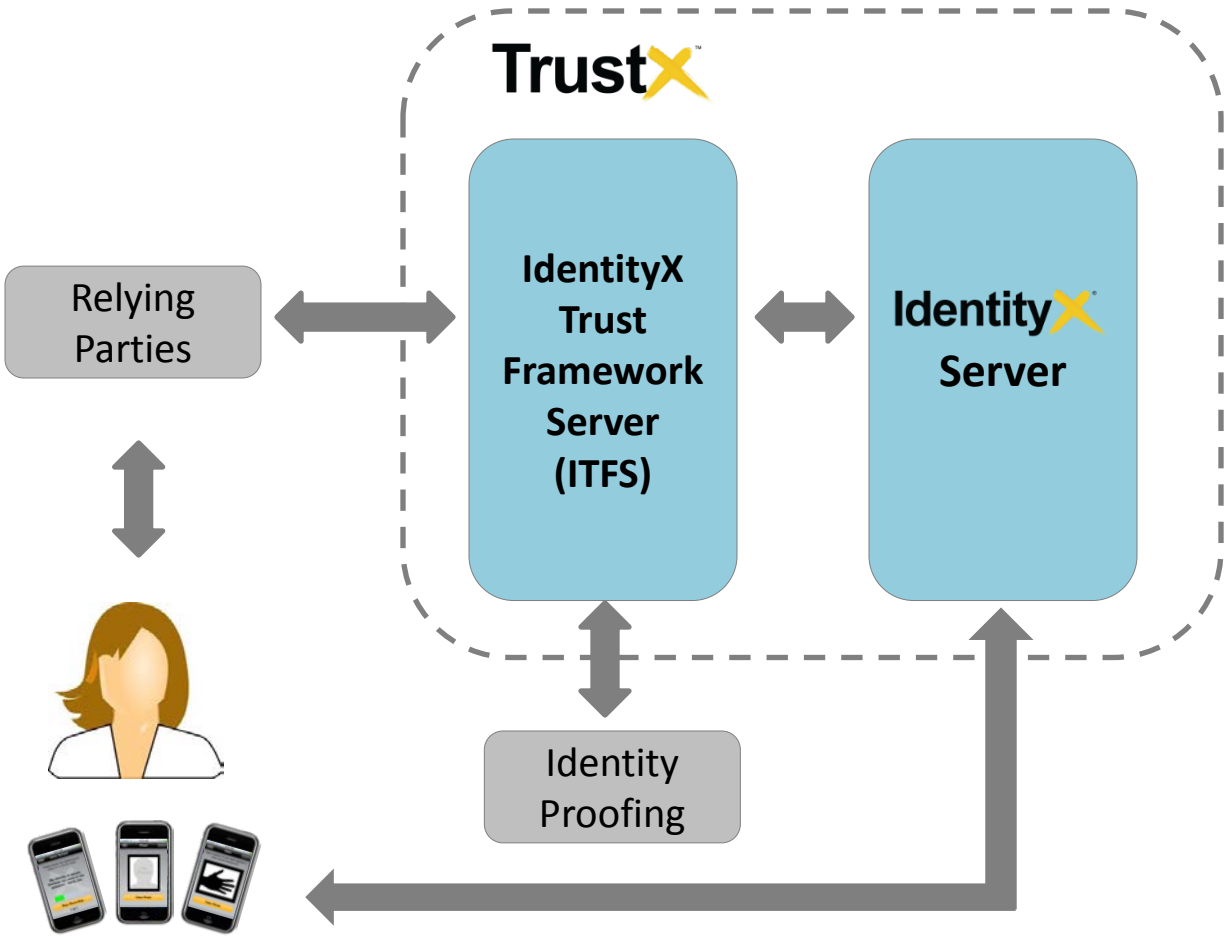
Identity Provider Service

- Full IDP service:
  - Identity proofing (via partner)
  - Hold min set of data
  - Credentialing
- Single credential can be bound by multiple RPs
- Support subscriber approved sharing of identity data
- LOA3 for all

Credential Service

- Strong credential issuance, management, verification
- RP performs ID proofing & holds identity data
- Process to bind credential to identity (sponsorship)
- RPs independently bind
- Single credential can be bound to multiple RPs

TrustX IDP Architecture

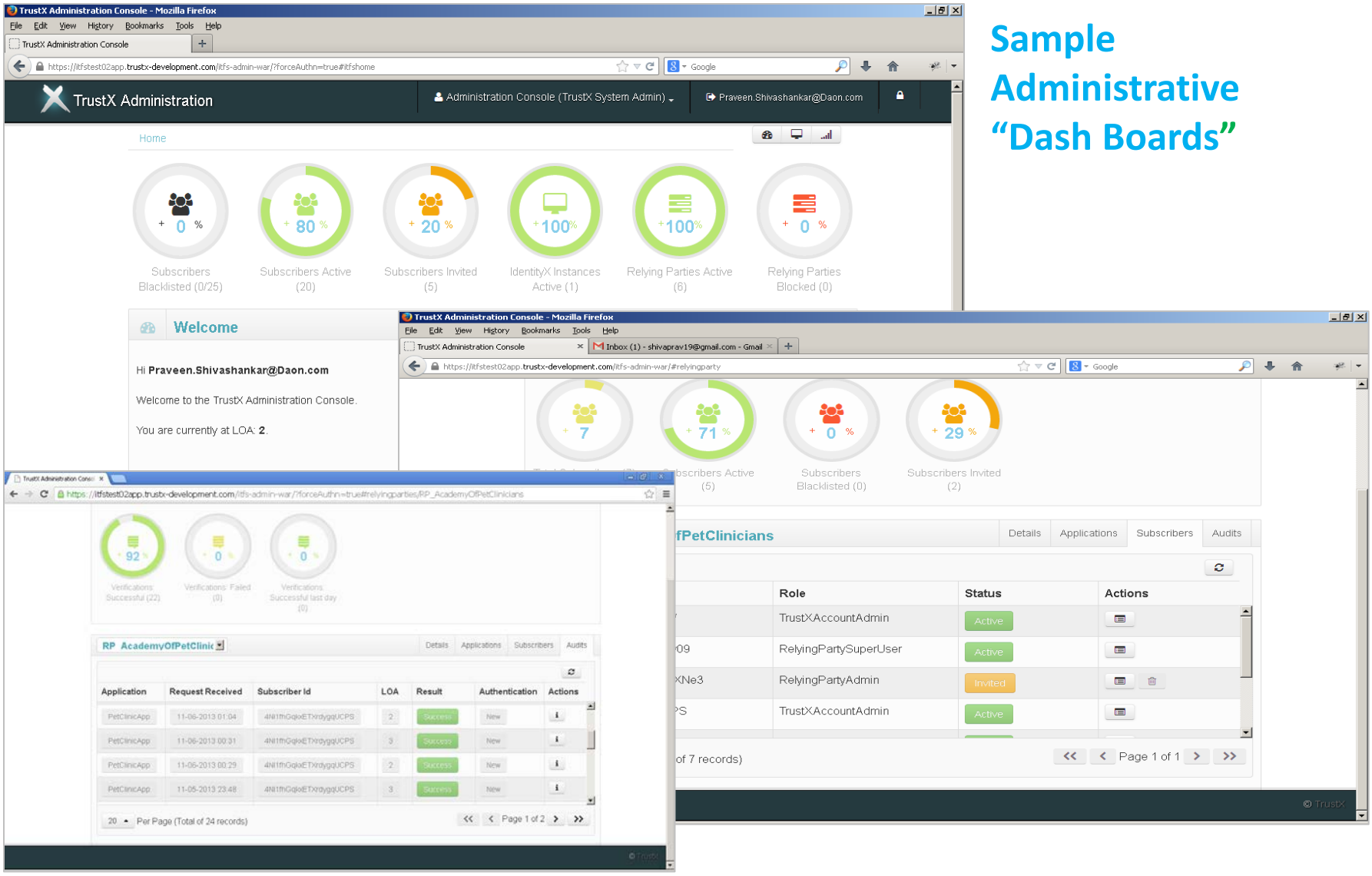


ITFS Capabilities

- Multi-tenancy
- Standard WebSSO interfaces
  - OpenID Connect & SAML2
- Sign-Up/Sign-On process
- ITFS & RP administration
  - RP onboarding
  - Lifecycle functions
- RP administrator portal
  - RP applications & subscribers
  - Sponsorship
  - Account blocking/unblocking
- Subscriber portal
  - Profile management
  - Self-service support (e.g., lost/new device)
- 3rd party identity proofing
- Transaction auditing

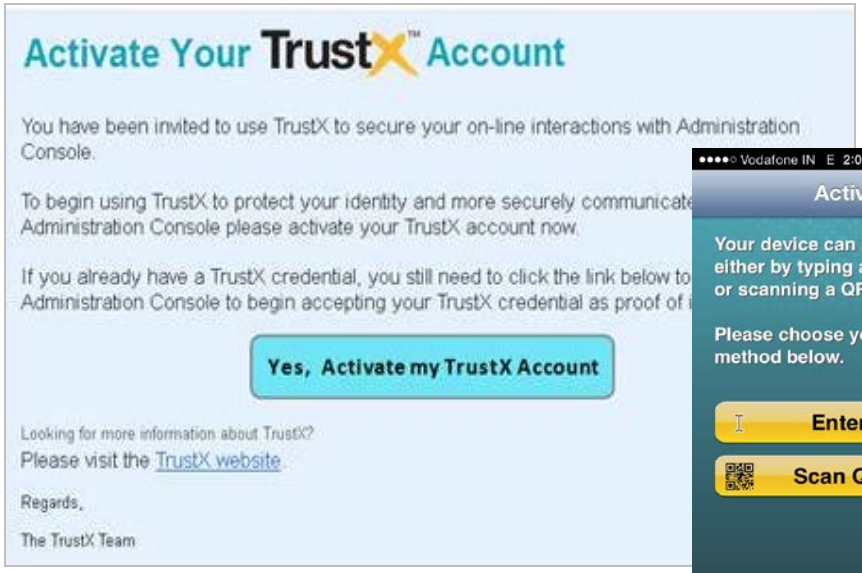
Proprietary and Confidential

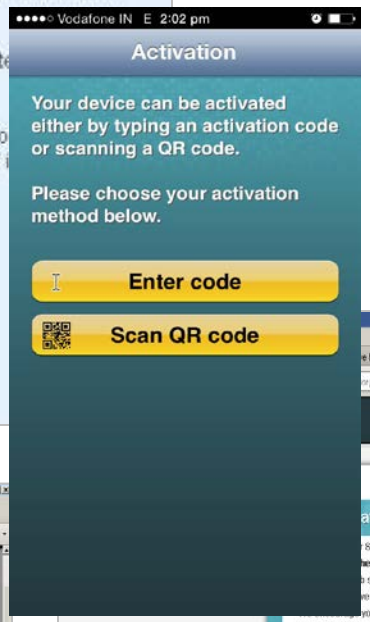
Technology - ITFS

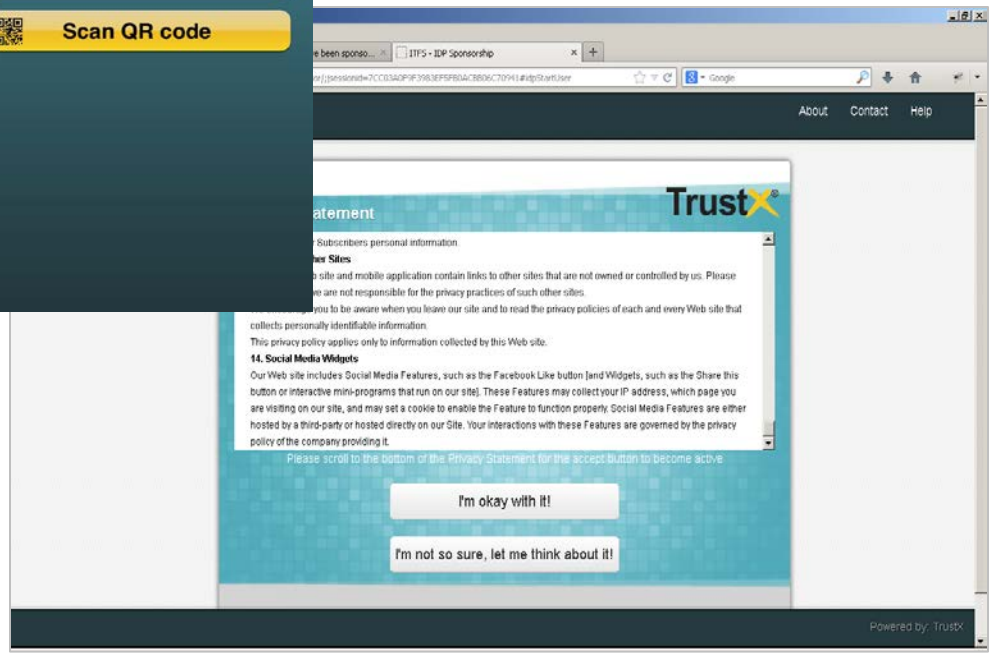


Sample Administrative "Dash Boards"

Technology - ITFS







Browser and Mobile Device Screen shots associated with enrollment . We will walk through this in some detail in a few minutes.

What is different about us?

- Dynamic risk based multifactor/multi-method
- Mobile authentication platform that users already have
- Non-traditional token types, including biometrics
- Trust elevation
- Equivalence
- Modular model – “full IDP” and “CSP only”
- Supporting multiple RP interfaces – SAML2 & OpenID Connect

Trust Frameworks – NSTIC Alignment

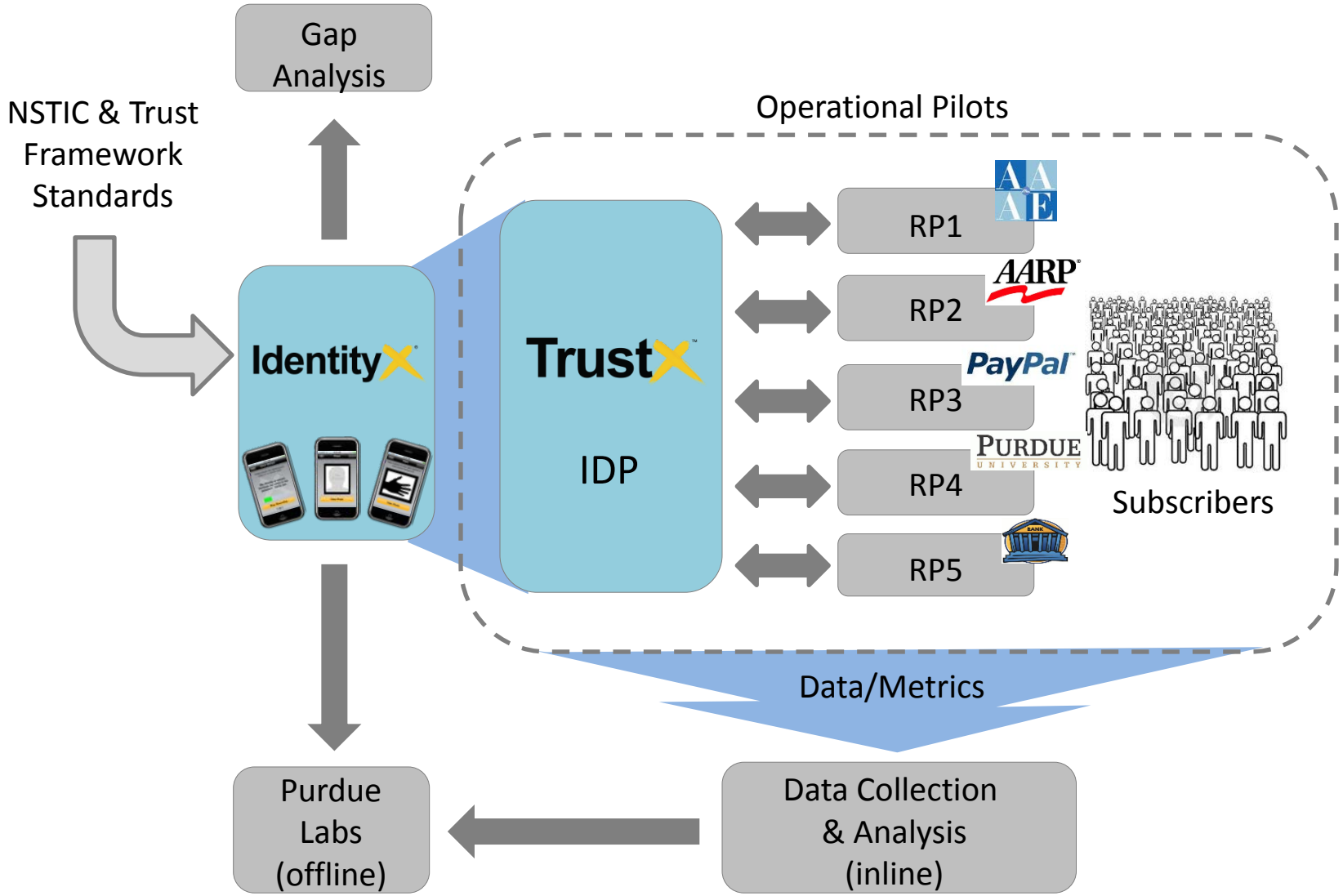
- Migrating our TrustX IDP to work within multiple trust frameworks
- Provides CHOICE to subscribers and Relying Parties
- Operate within a multiple IDP environment
- Will assess existing trust frameworks to support:
  - Risk-based multi-factor/multi-method
  - Trust elevation
  - Biometrics
  - Equivalence

Research – Purdue University

- Biometric Standards, Performance & Assurance Laboratory (BSPA)
- Center for Education and Research in Information Assurance and Security (CERIAS)
- Practical research
  - Offline - Laboratory
  - Online – Analyzing data from the operational pilots
- Areas
  - Usability
  - Accessibility
  - Privacy
  - Security
  - Performance
  - User acceptance

Operational Pilots

Daon



Steps to get there

- Extend the technology to fit within federated environment and meet certification criteria
  - Involves requirements analysis & trade-offs
  - Supported by research assessments
  - Identify gaps in existing TF standards along the way
- Stand up the enhanced IDP/CSP
- Integrate RP applications
  - Work with RPs on pilot plans (use cases, populations, approaches, schedule, etc.)
- Work through Trust Framework certification and back fit RP integrations to align
  - Work with assessors and consultants
- Collect and analyze metrics to evaluate progress, success
- Work with other pilots to identify opportunities to work together

Lessons Learned (so far)

- RP adoption challenges
- Componentized identity models still in their infancy
- Methods do not exist for assessing equivalency of token types
- Conformance to standards inhibits some functionality
- Privacy enhancements can sometimes add business difficulties
- Interoperable credentials have non-obvious implications
- Lack of standards around some critical processes/interfaces
- Standards are biased towards hard tokens and secrets
- Standard interfaces/profiles not targeted at 'in-band' applications
- Standards/trust frameworks don't seem to acknowledge that someone has to pay
- Immaturity of some standards
- Standards not keeping pace with market demands

See 16 Dec IDESG report out for more details:
https://www.idecosystem.org/filedepot_download/1369/1039

Proprietary and Confidential

Use Cases

- General use case:
  - Relying party has an existing relationship with a set of subscribers (customers, members, partners, staff, etc.)
  - RP wants a strong authentication solution (credential) for its higher assurance applications/transactions
    - RP maps its transactions to a set of authentication methods (low to high)
  - RP is willing to use (try using) an external service
    - RP may operate within a trust framework/federation
  - In general, the RP performs its own identity proofing and holds identity data, which is bound to the strong credential
    - However some RPs may desire to also utilize 3rd party identity proofing, particularly for new subscribers
  - RPs sponsor a subscriber for a TrustX credential; however once issued, this credential may be bound to multiple RPs
  - Subscriber uses their credential in lieu of passwords

Proprietary and Confidential

Use cases

Daon

Relying Party	Use Case	Pilot Population	Potential Base	Notes
AAAE	Member portal access	AAAE members	5000	Ability to pilot different subsets of population with different access concerns
AARP	PHR	Members	40M	Focus likely to be more on usability than security
Purdue	Passport (OpenBadge)	Students/ Faculty	85K	Year 2 pilot
Major Bank	On-line and mobile banking	Bank customers	50M	Year 2 pilot
PayPal	eCommerce	Under NDA	TBD M	Year 2 pilot

Proprietary and Confidential

AARP's Goals for the NSTIC Pilot

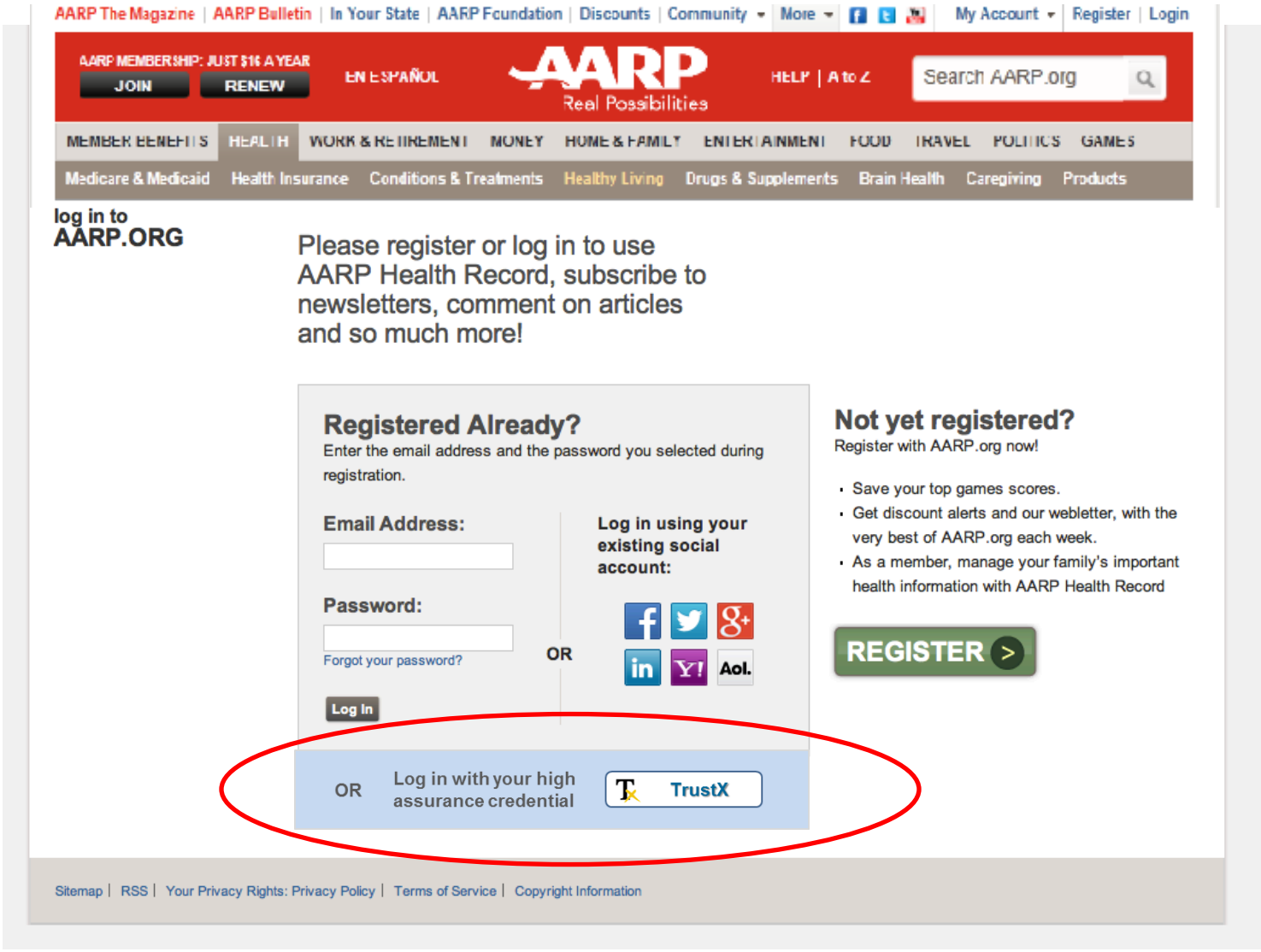
- Improve members' online experience
- Facilitate new services requiring higher levels of identity assurance
- Protect member information
- Reduce the number of individual identity credentials required
- Give more control to the individual (member)
- Support family and inter-generational applications
- Investigate usability and user acceptance

AARP Use Case

AARP Health Record (SM)

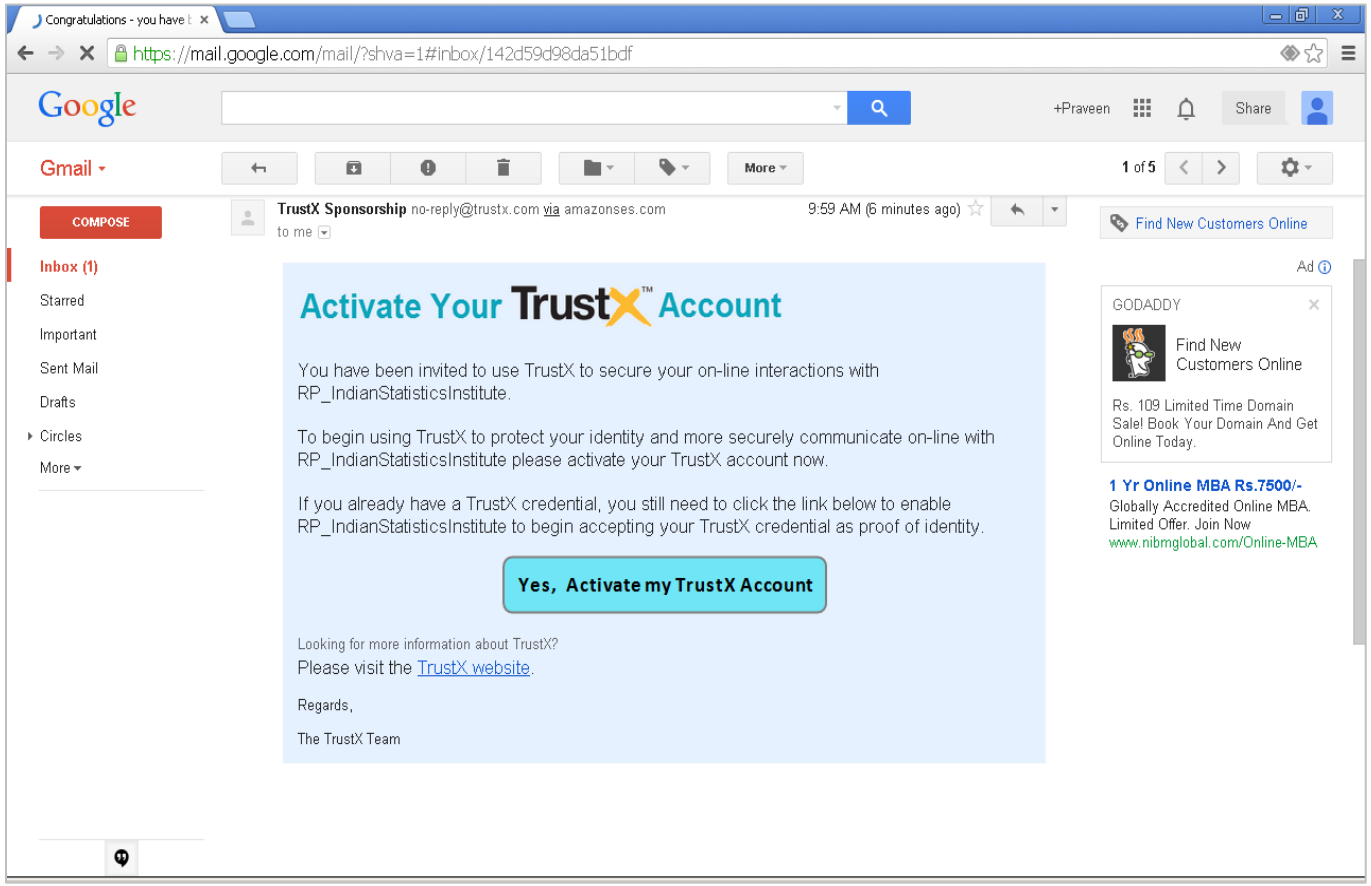
- An easy-to-use, online tool designed to help people over 50 manage their family health care needs.
- Lets you safely store and access critical health information such as medications, allergies, blood type, immunizations and emergency and provider contact information.
- Lets you print an easy-to-read pocket card with vital stats. You can also quickly access your family's health information from any computer, mobile phone or tablet.
- (May be particularly relevant in certain geographic regions, i.e., Gulf Coast, Tornado Alley, etc.)
- Helps you prepare for emergencies by allowing you to store your family's health information in one easy-to-access location.
- Is free to AARP members. It is available at www.aarp.org/healthrecord and http://www.aarp.org/mihistorialdesalud.
- Connects with Microsoft HealthVault, a security- and privacy-enhanced online data repository that enables users to organize, store, share and use their personal health information as desired.

AARP Use Case – Health Record Access



AARP Use Case – Health Record Access

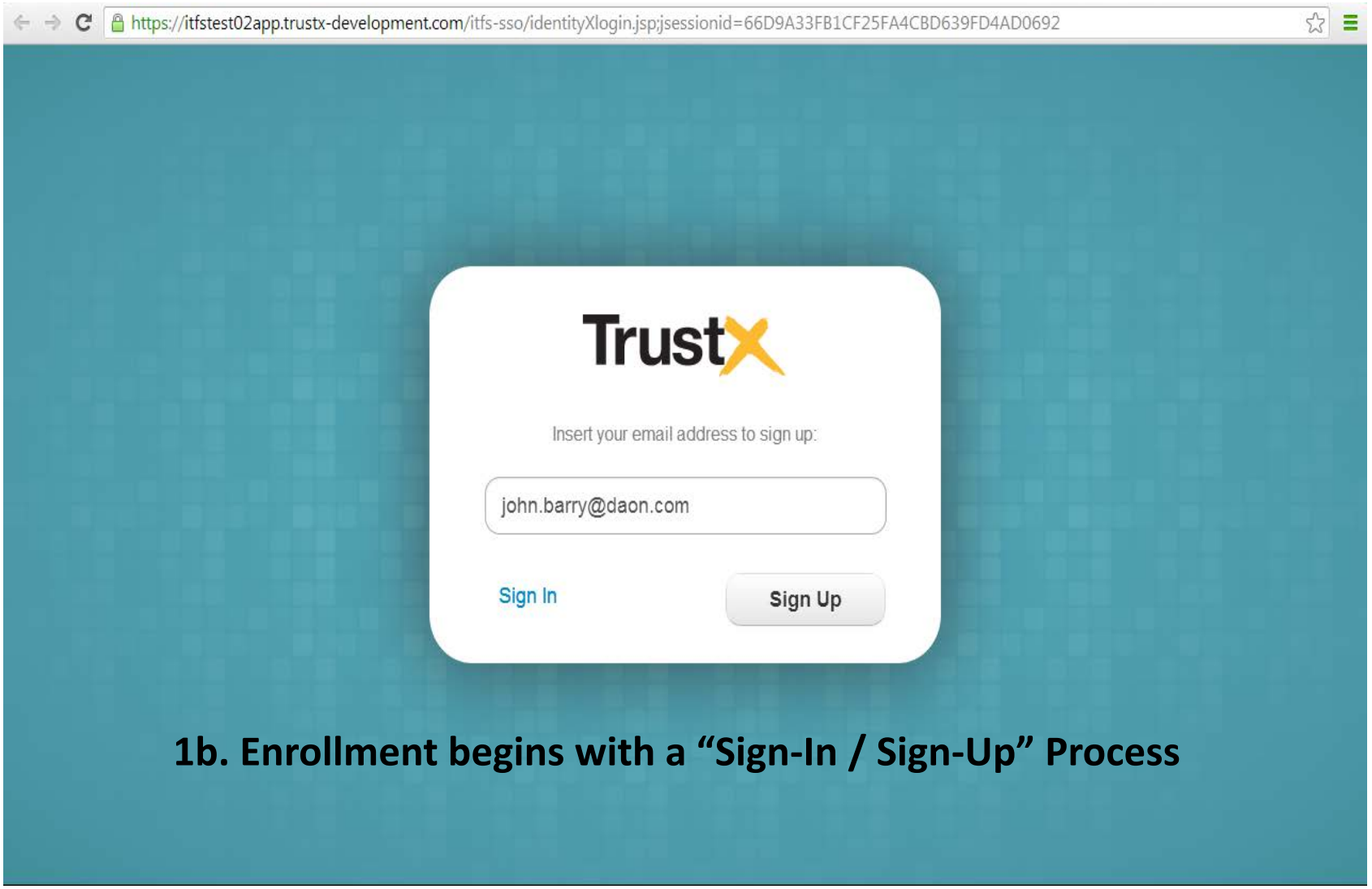
Enrollment



1a. Enrollment begins with a "Sponsorship Email" OR …

AARP Use Case – Health Record Access

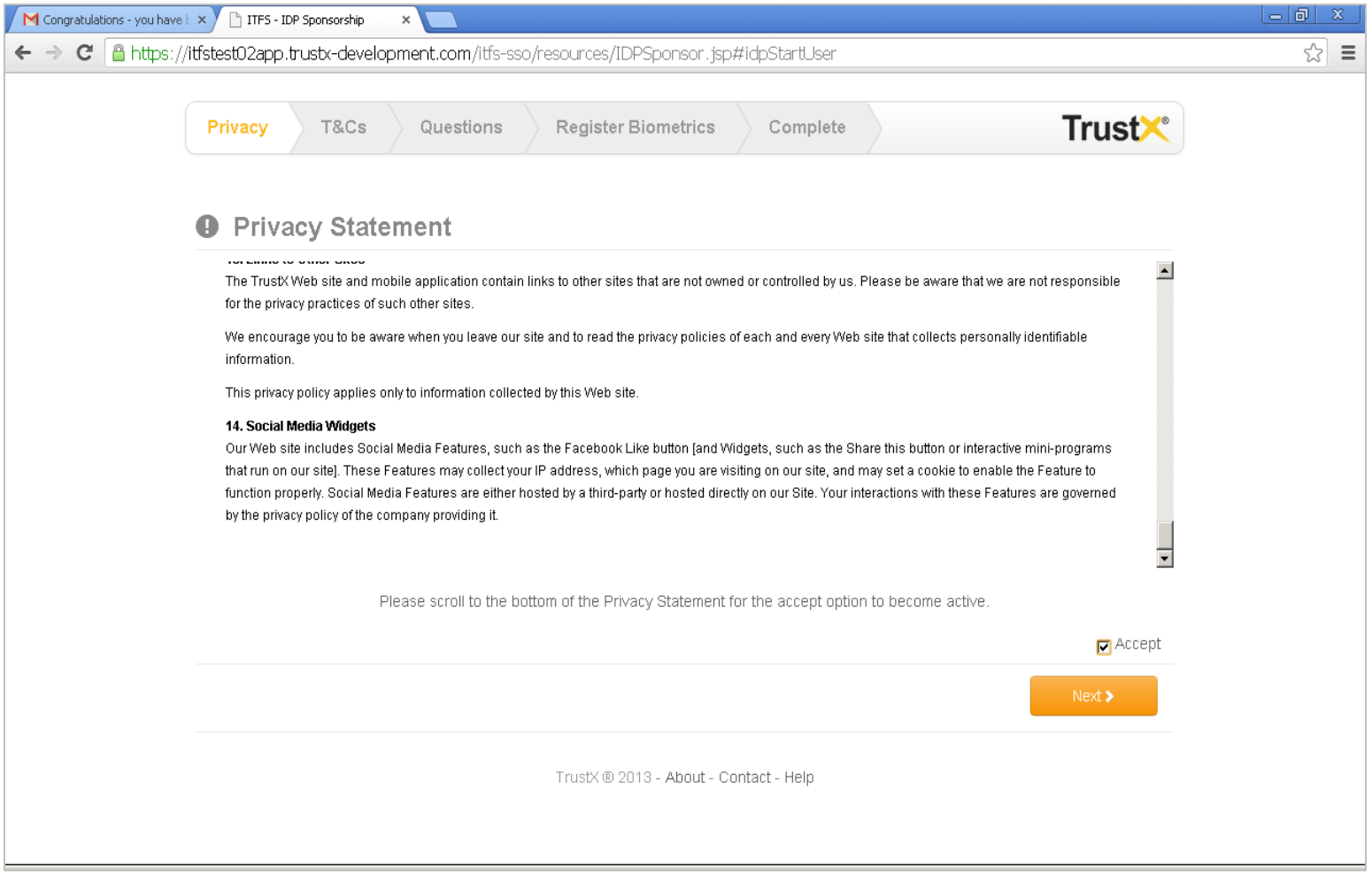
Enrollment



1b. Enrollment begins with a "Sign-In / Sign-Up" Process

AARP Use Case – Health Record Access

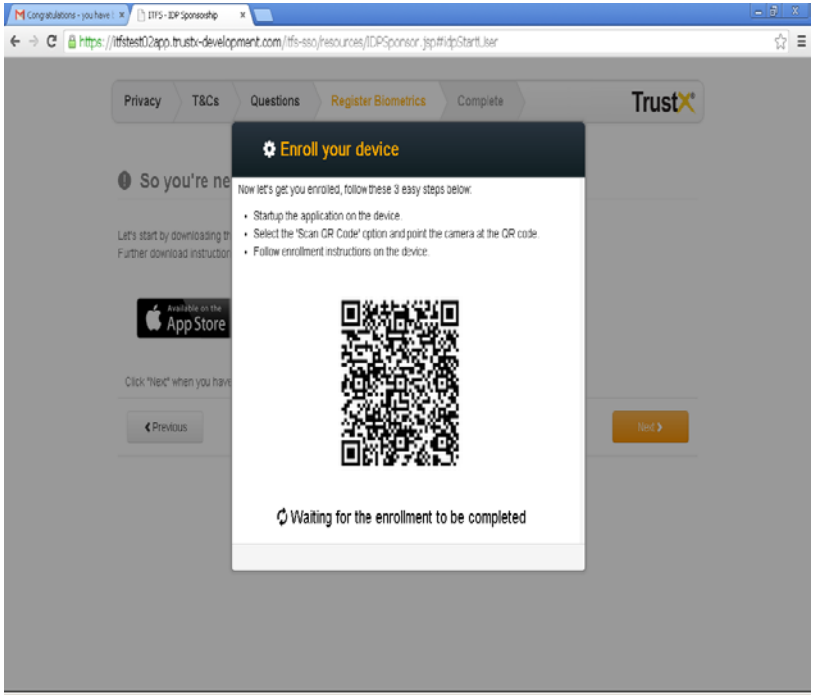
Enrollment



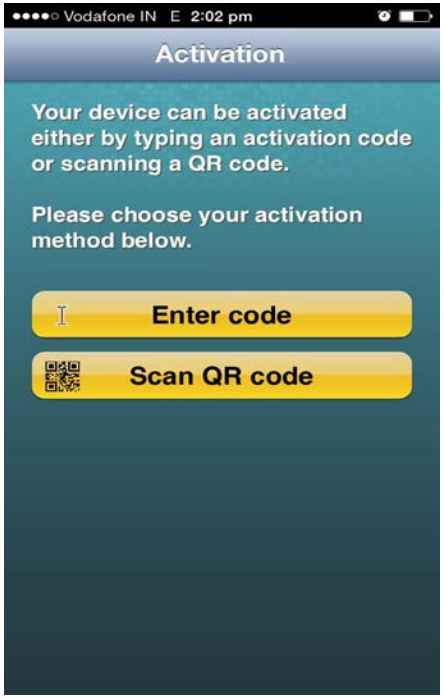
2. Accept TrustX Privacy Policy and Terms and Conditions of Use

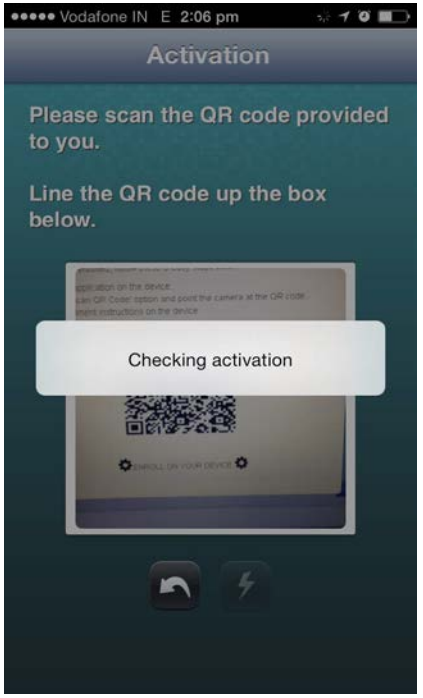
AARP Use Case – Health Record Access

Enrollment



Browser





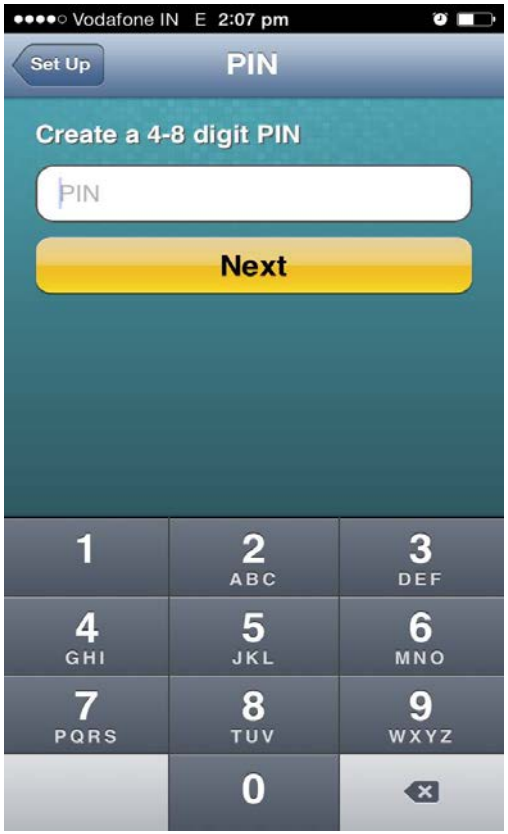
Applicant's Mobile

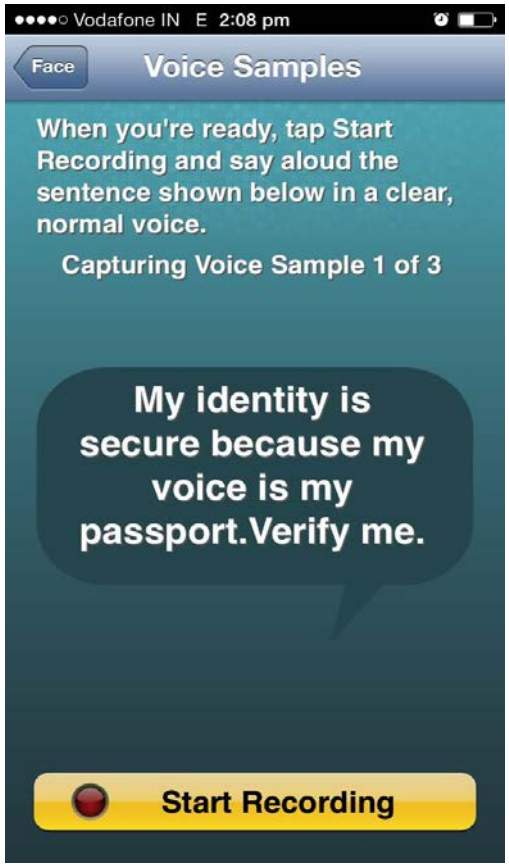
3. Download TrustX Authenticator APP

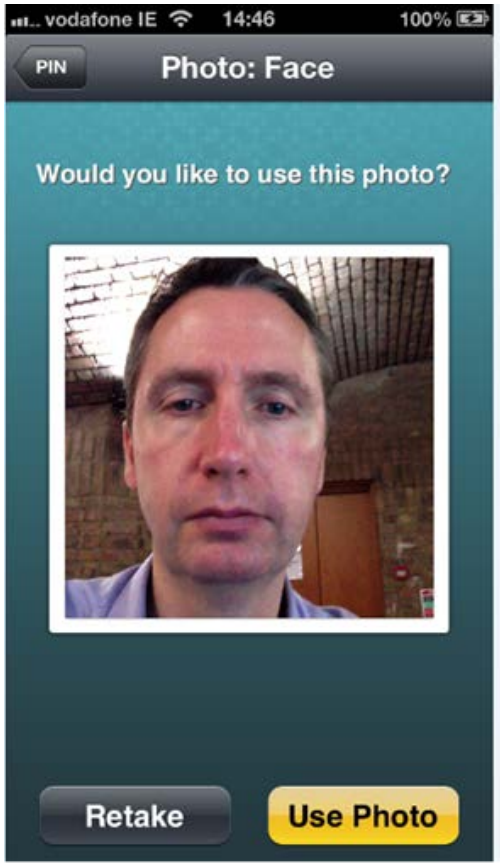
4. Scan the QR code with the APP to link the enrollment record to the device

AARP Use Case – Health Record Access

Enrollment



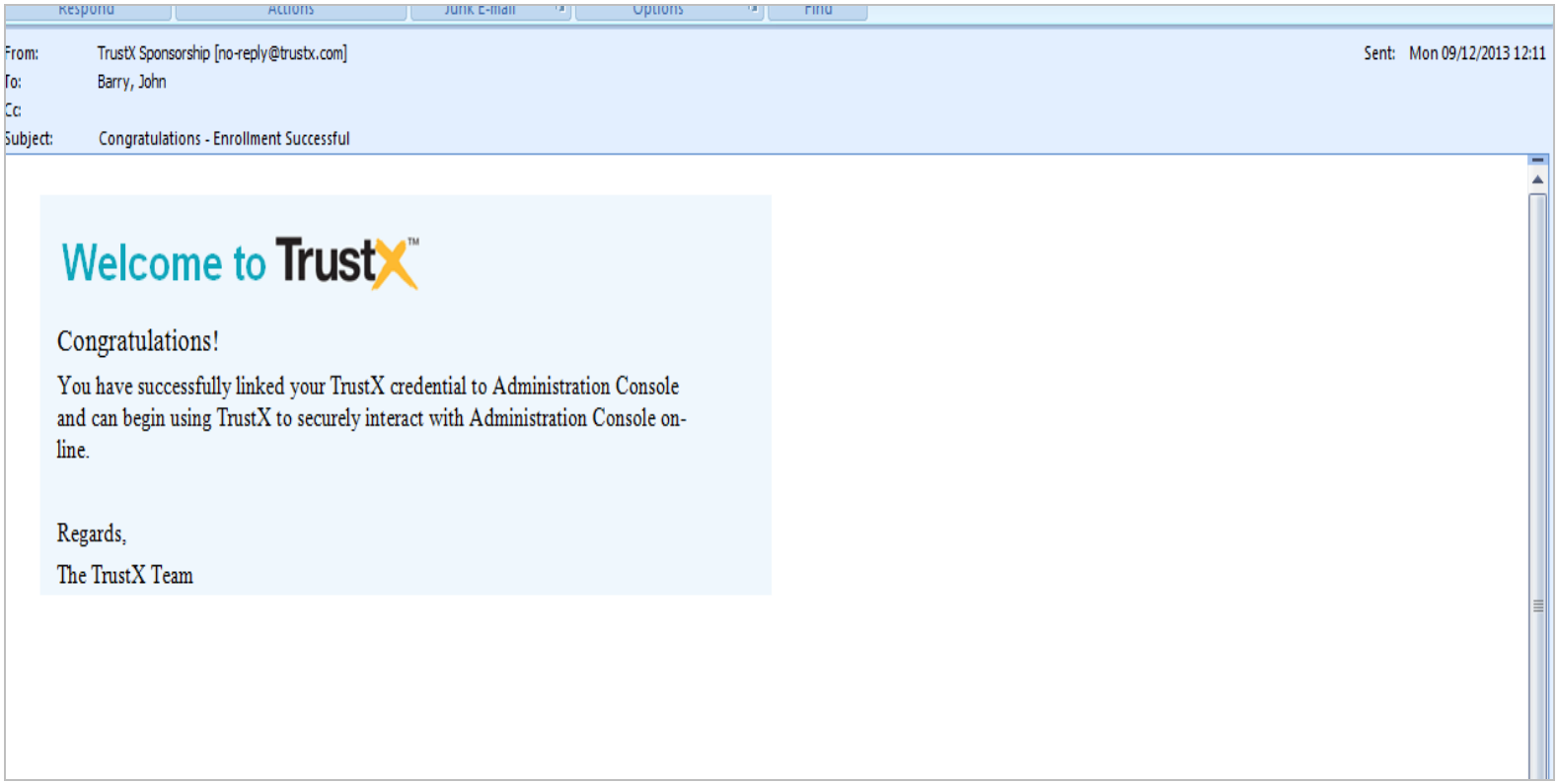




5. Select a PIN
6. Enroll Biometrics (Face and Voice)

AARP Use Case – Health Record Access

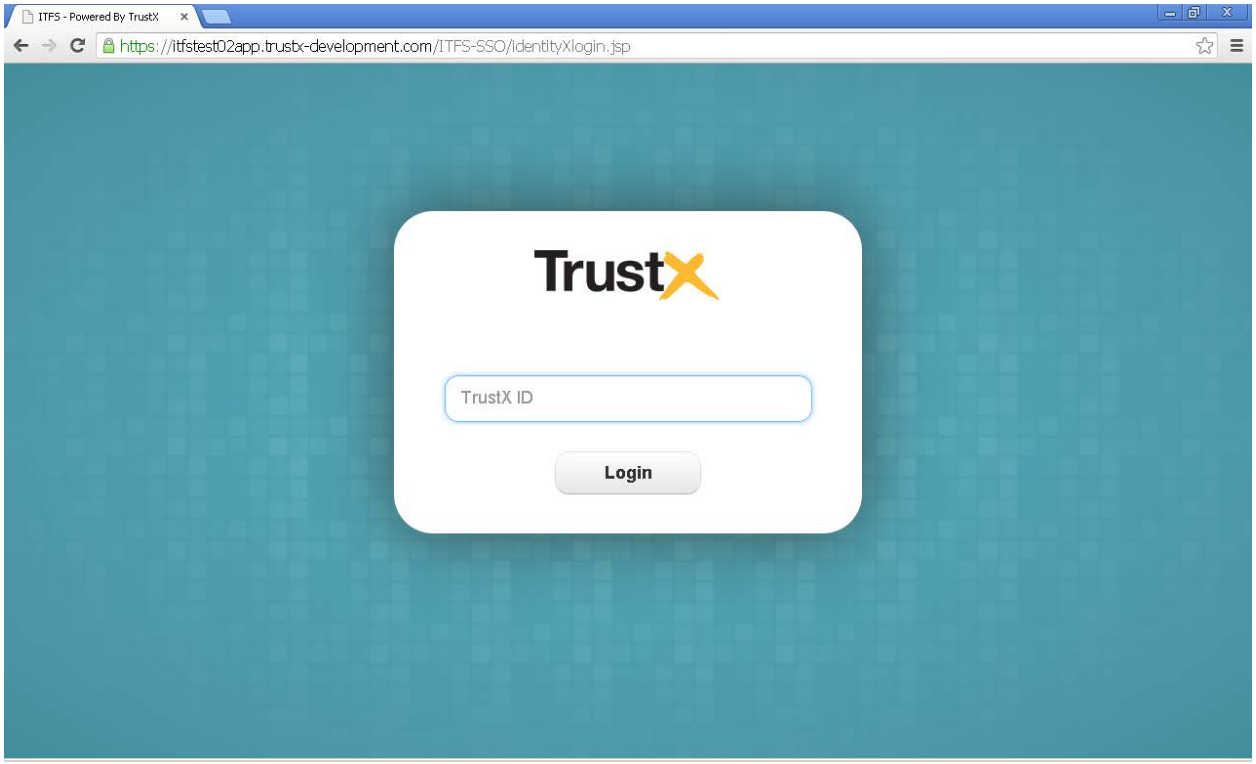
Enrollment



7. Welcome email

AARP Use Case – Health Record Access

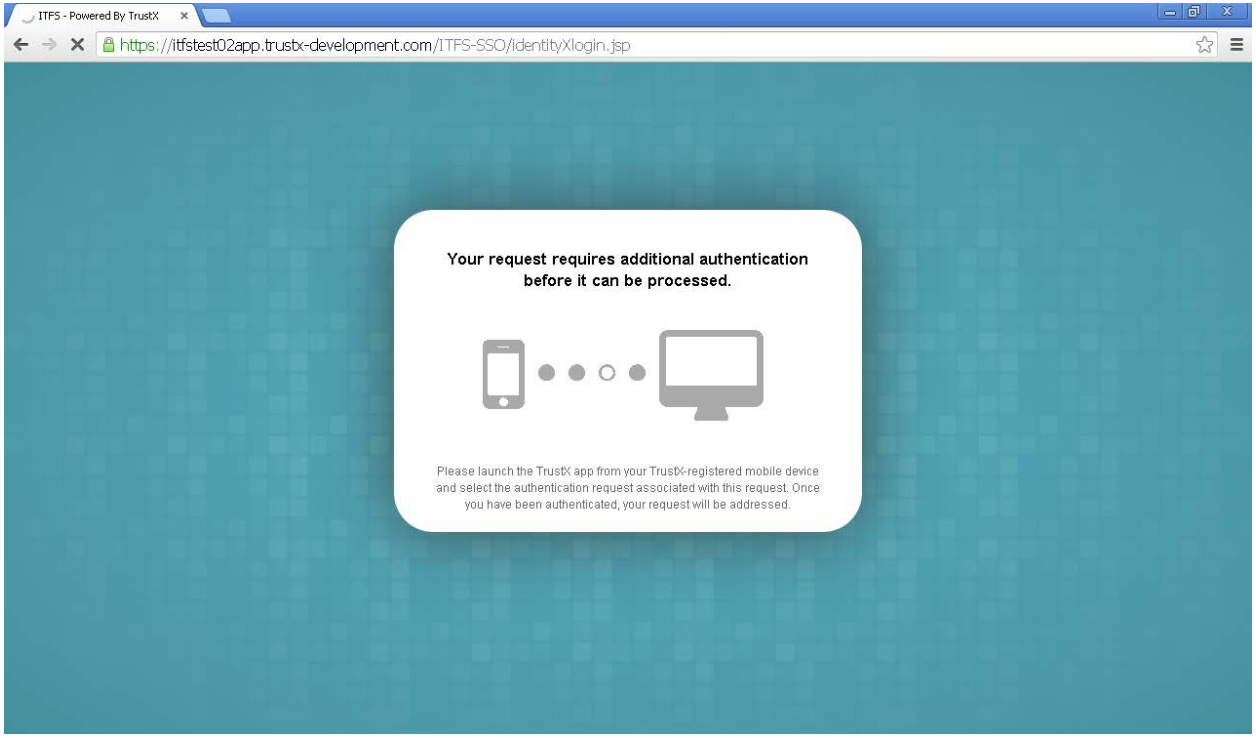
Usage



1. **Subscriber enters their TrustX ID (e.g. their email address)**

AARP Use Case – Health Record Access

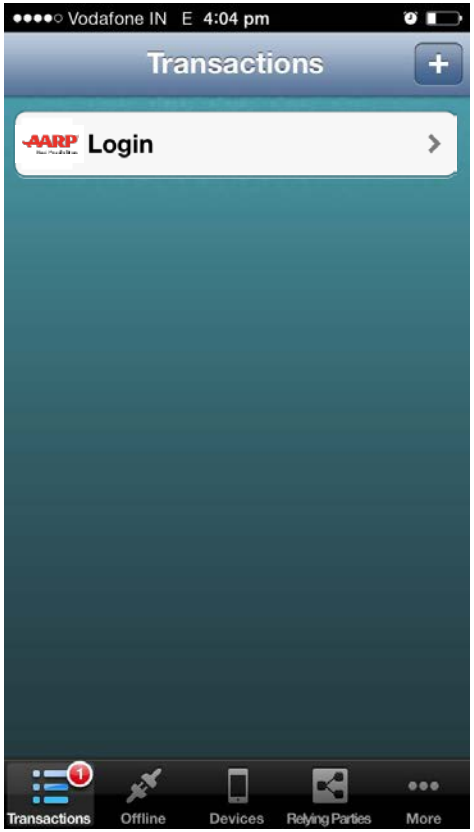
Usage

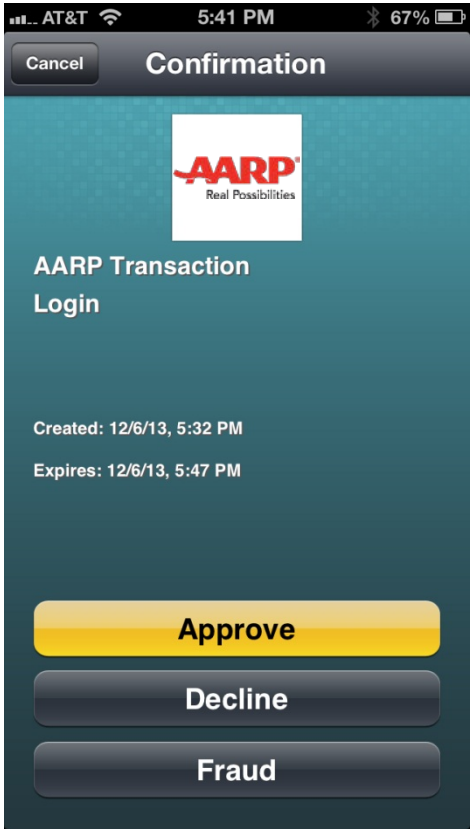


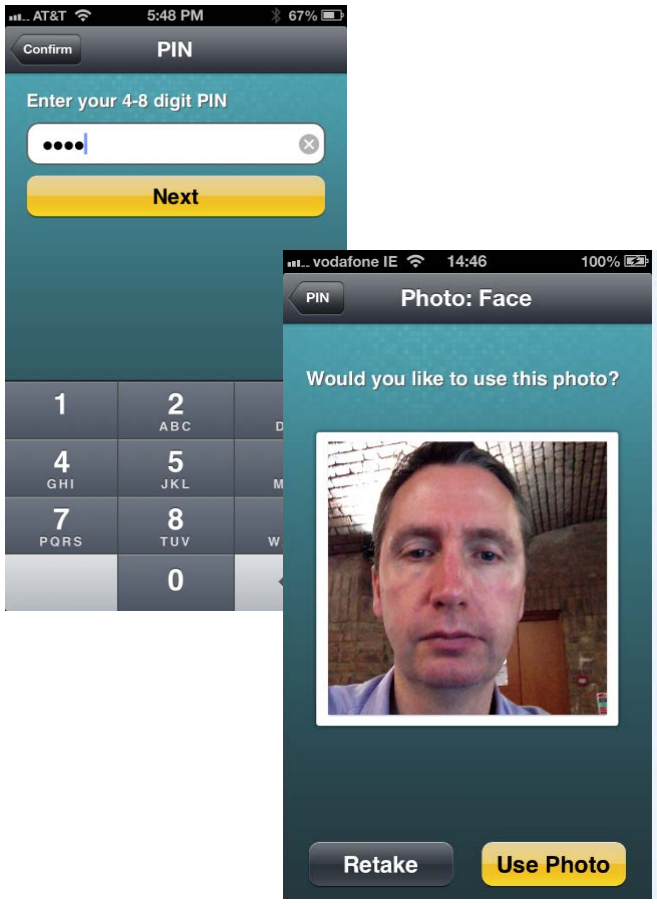
2. Based on Relying Party authentication policies, TrustX sends authentication challenges to the Subscribers mobile

AARP Use Case – Health Record Access

Usage

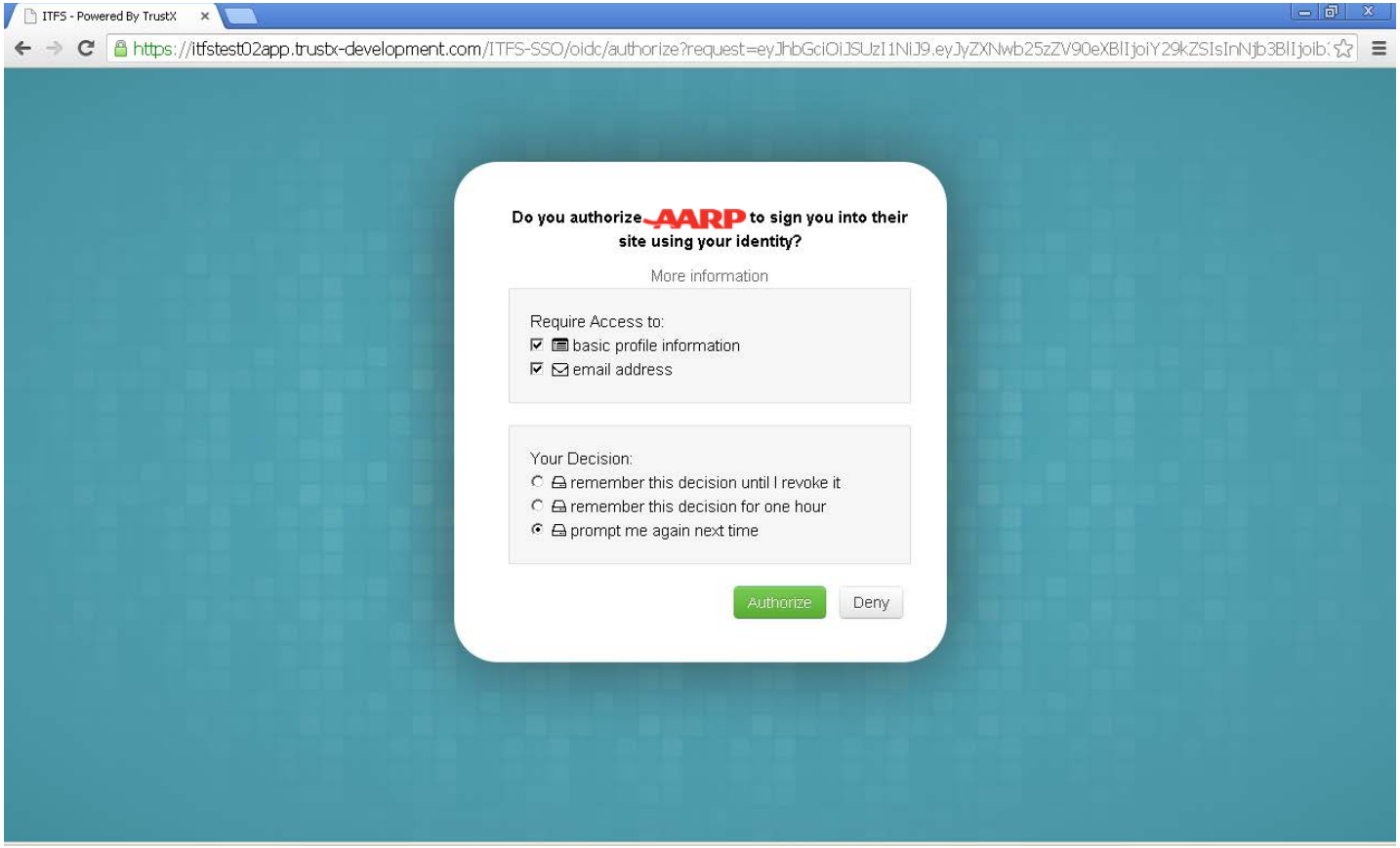






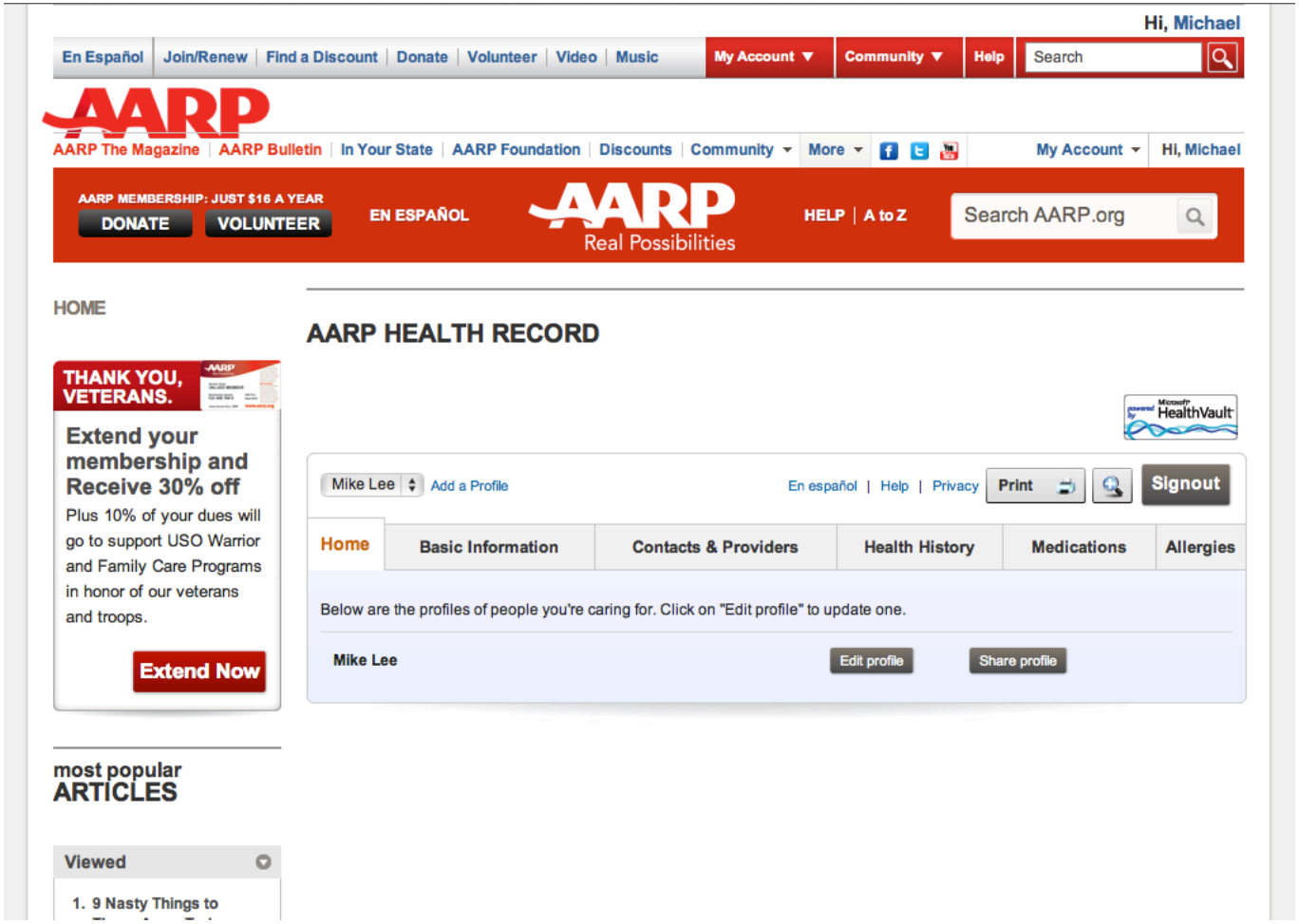
3. Subscriber opens APP to view pending transactions
4. Approves the AARP Log-in
5. Responds to authentication challenges (PIN and/or Face and/or Voice)

AARP Use Case – Health Record Access



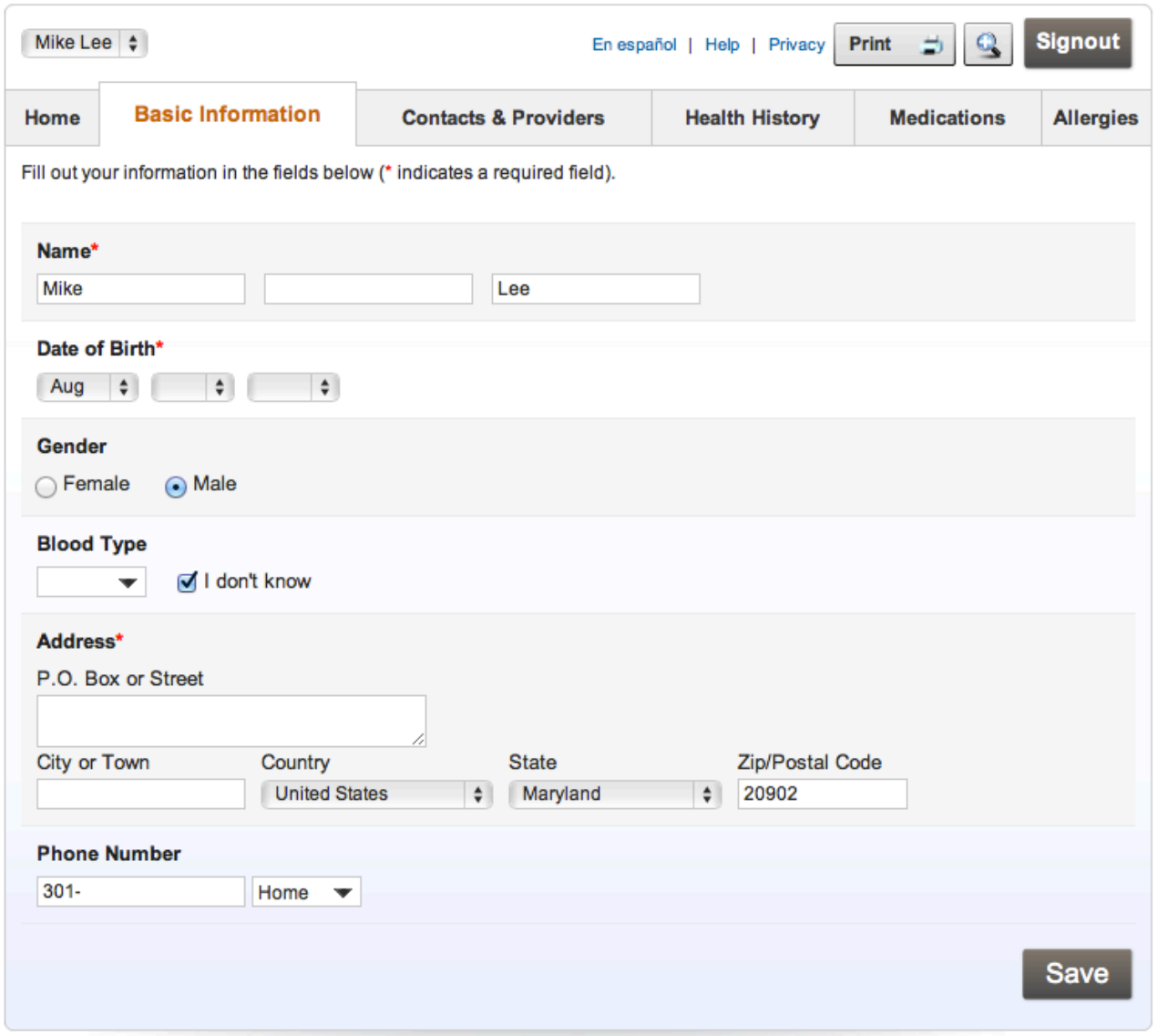
6. Subscriber determines what information they will / will not share with the Relying Party. (Note: The Subscriber can set a default policy so they don't need to perform this step each time).

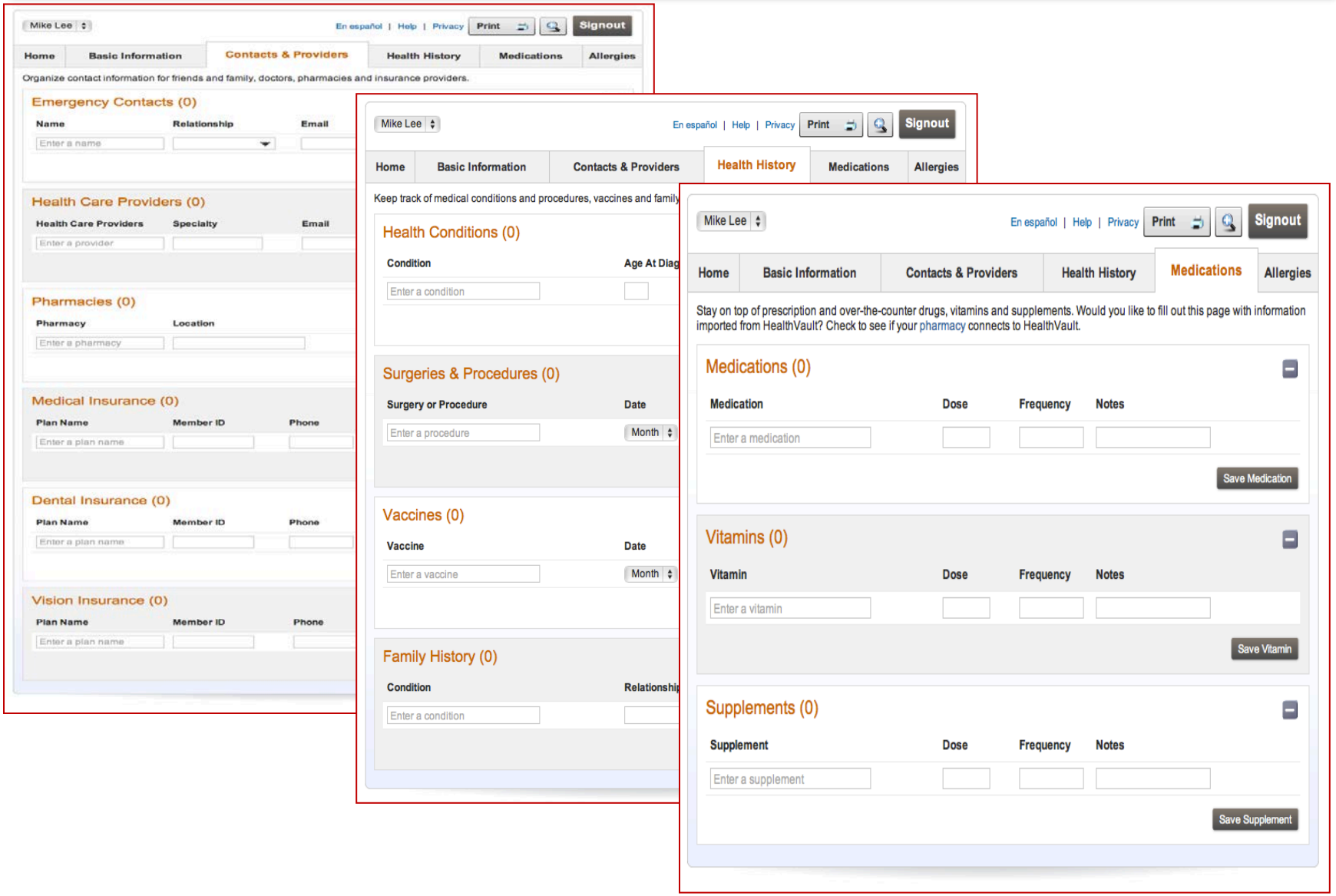
AARP Use Case – Health Record Access



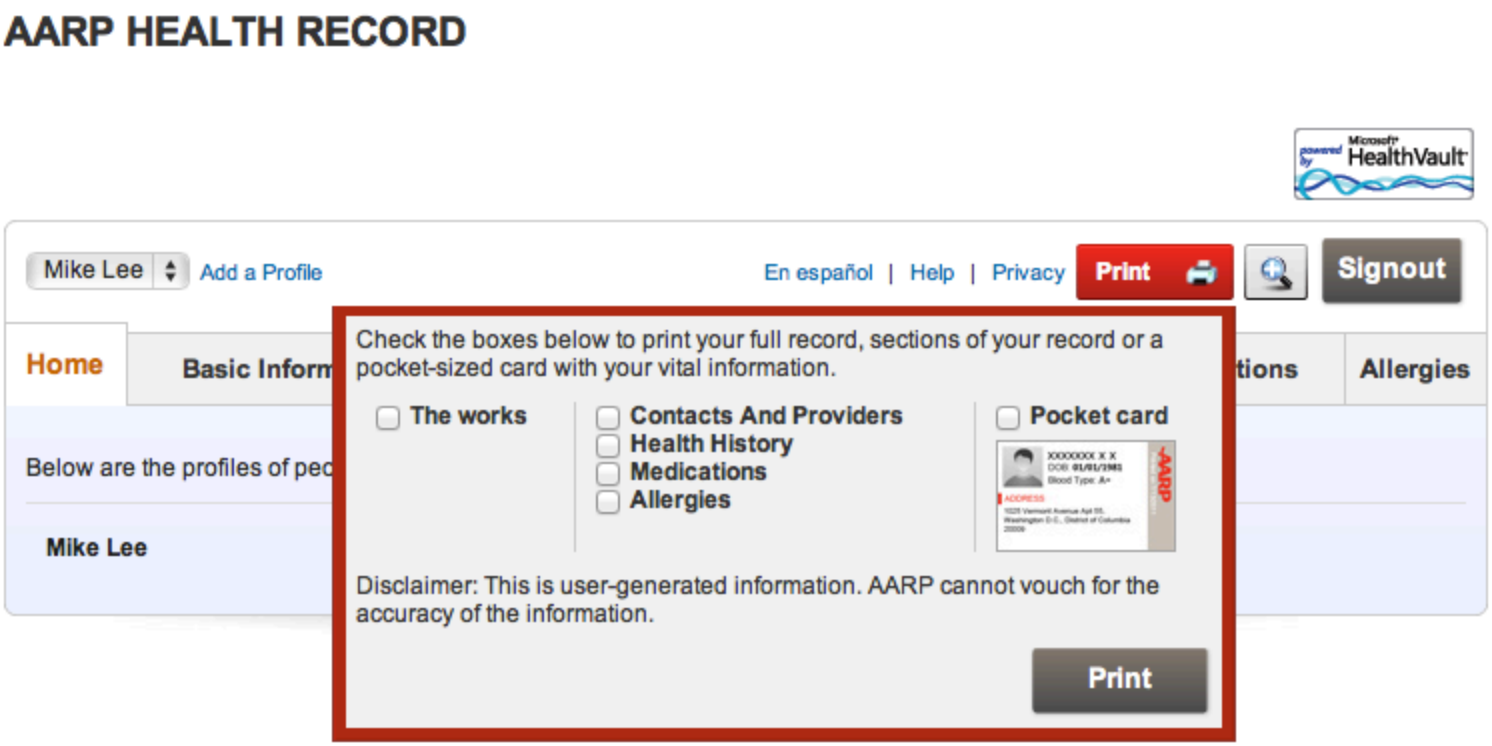
7. TrustX returns subscribers "identity information" to RP which then makes the access decision.

AARP Use Case – Health Record Access

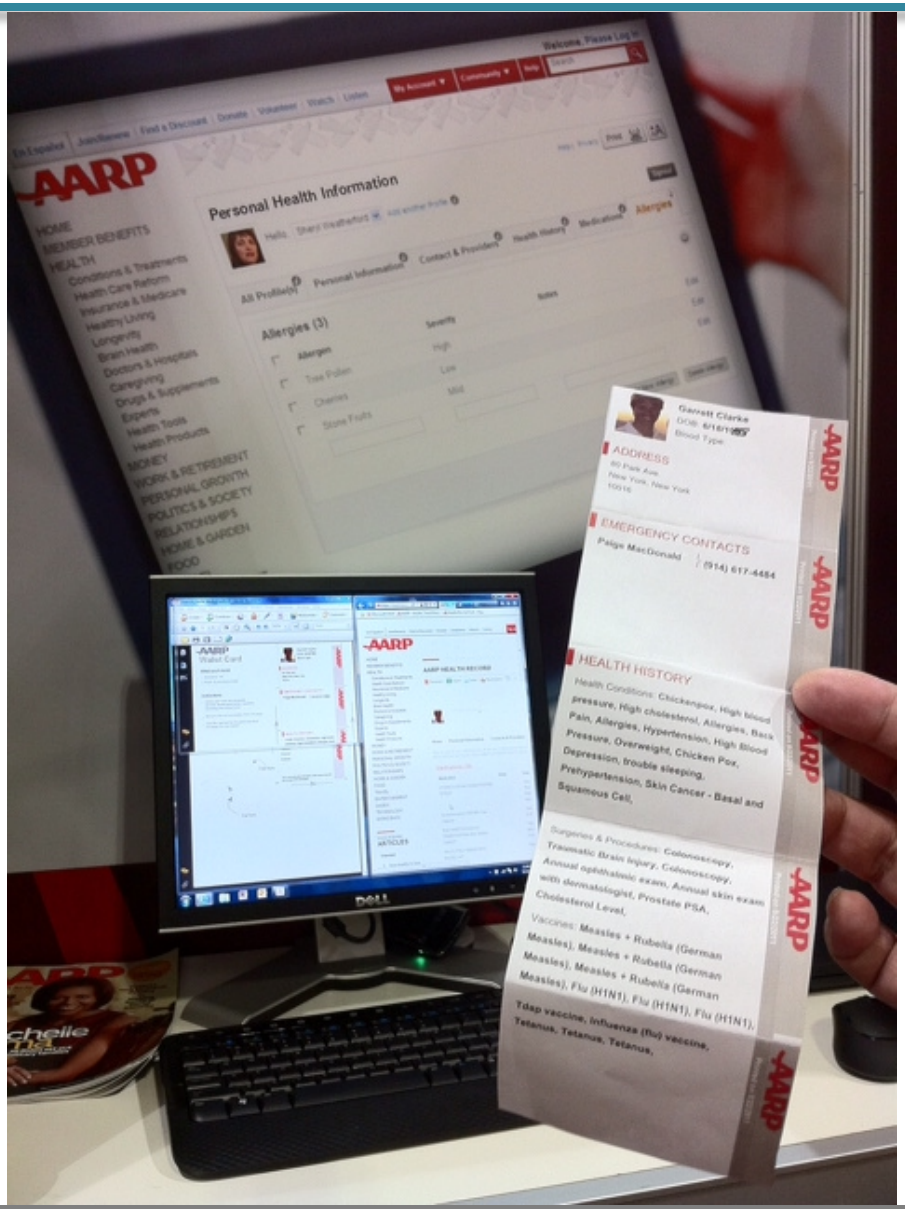



Mike Lee
En español | Help | Privacy
Print
Signout
Home
Basic Information
Contacts & Providers
Health History
Medications
Allergies
Organize contact information for friends and family, doctors, pharmacies and insurance providers.
Emergency Contacts (0)
Name
Relationship
Email
Enter a name
Health Care Providers (0)
Health Care Providers
Specialty
Email
Enter a provider
Pharmacies (0)
Pharmacy
Location
Enter a pharmacy
Medical Insurance (0)
Plan Name
Member ID
Phone
Enter a plan name
Dental Insurance (0)
Plan Name
Member ID
Phone
Enter a plan name
Vision Insurance (0)
Plan Name
Member ID
Phone
Enter a plan name
Mike Lee
En español | Help | Privacy
Print
Signout
Home
Basic Information
Contacts & Providers
Health History
Medications
Allergies
Keep track of medical conditions and procedures, vaccines and family
Health Conditions (0)
Condition
Age At Diag
Enter a condition
Surgeries & Procedures (0)
Surgery or Procedure
Date
Enter a procedure
Month
Vaccines (0)
Vaccine
Date
Enter a vaccine
Month
Family History (0)
Condition
Relationship
Enter a condition
Mike Lee
En español | Help | Privacy
Print
Signout
Home
Basic Information
Contacts & Providers
Health History
Medications
Allergies
Stay on top of prescription and over-the-counter drugs, vitamins and supplements. Would you like to fill out this page with information imported from HealthVault? Check to see if your pharmacy connects to HealthVault.
Medications (0)
Medication
Dose
Frequency
Notes
Enter a medication
Save Medication
Vitamins (0)
Vitamin
Dose
Frequency
Notes
Enter a vitamin
Save Vitamin
Supplements (0)
Supplement
Dose
Frequency
Notes
Enter a supplement
Save Supplement

AARP Use Case – Health Record Access



AARP Use Case – Health Record Access



AARP Use Case – Health Record Access

Take control of your health

Microsoft HealthVault is a trusted place for people to gather, store, use, and share health information online.

Learn more

You can also sign in with: Facebook OpenID TrustX

HealthVault

Because you're accessing sensitive info, you need to verify your password.

curiouslee@gmail.com

Password

Sign in

Can't access your account?

Sign in with a different Microsoft account

©2013 Microsoft Terms Privacy & Cookies Help Center Feedback

Purdue – Passport Application

Use Case – Passport

- Learning system that demonstrates academic achievement through customizable badges
- Integrates with Mozilla OpenBadges
  - Using this infrastructure, any organization can use, create, and issue these badges
- Purdue has extended their existing Passport application to allow for multiple authentication options – e.g., FaceBook Connect
  - They are now integrating with TrustX
- 1st phase pilot
  - Class: IT34500, Automatic Identification and Data Capture
  - Badge: NSTIC 101
- Links:
  - http://www.itap.purdue.edu/studio/
  - Video: http://www.youtube.com/watch?v=O41-BWJ_VE0
  - http://openbadges.org/quickstart/

Proprietary and Confidential

Purdue – Passport Application

Purdue – Passport Application

Apply for Beta

Purdue is accepting **test pilot applications** for a limited number of beta users so that instructors everywhere can explore **digital badges for learning**.

Apply now.

Badge–powered flexible learning

Passport guides students through tasks by providing a framework to submit documents, share links, complete quizzes, or gather approvals. Instructors can follow each student's progress and connect badges with course objectives.

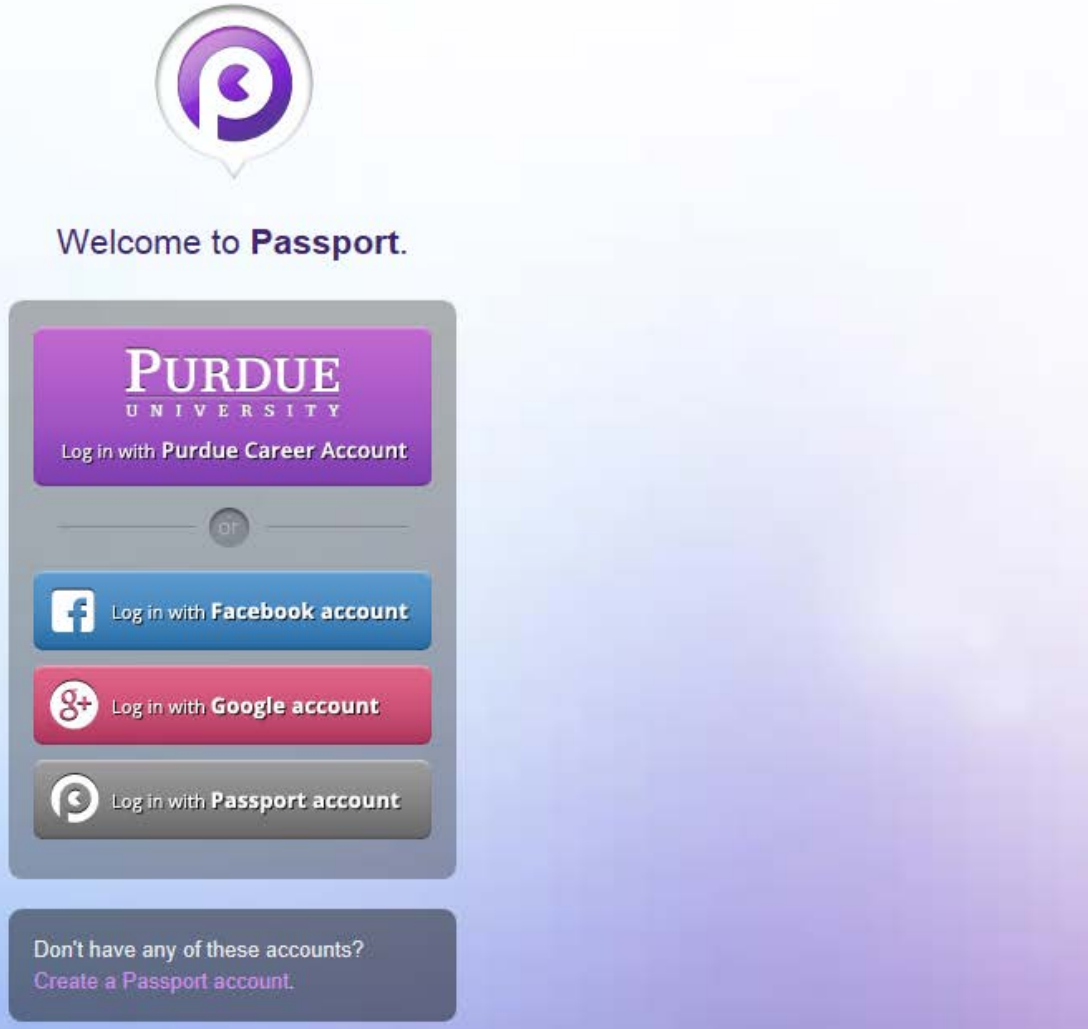
Badge builder

With the system's badge-builder tool, instructors can select different styles, colors, icons and fonts for each badge, or upload their own images. They also can set expiration dates for challenges, or reset tasks when a student's first attempt is not satisfactory.

Scorecard

Achievements — such as essays, online discussions, blog posts and podcasts, to name a few — can then be translated into a numeric-based evaluation system for grading purposes.

Purdue – Passport Application

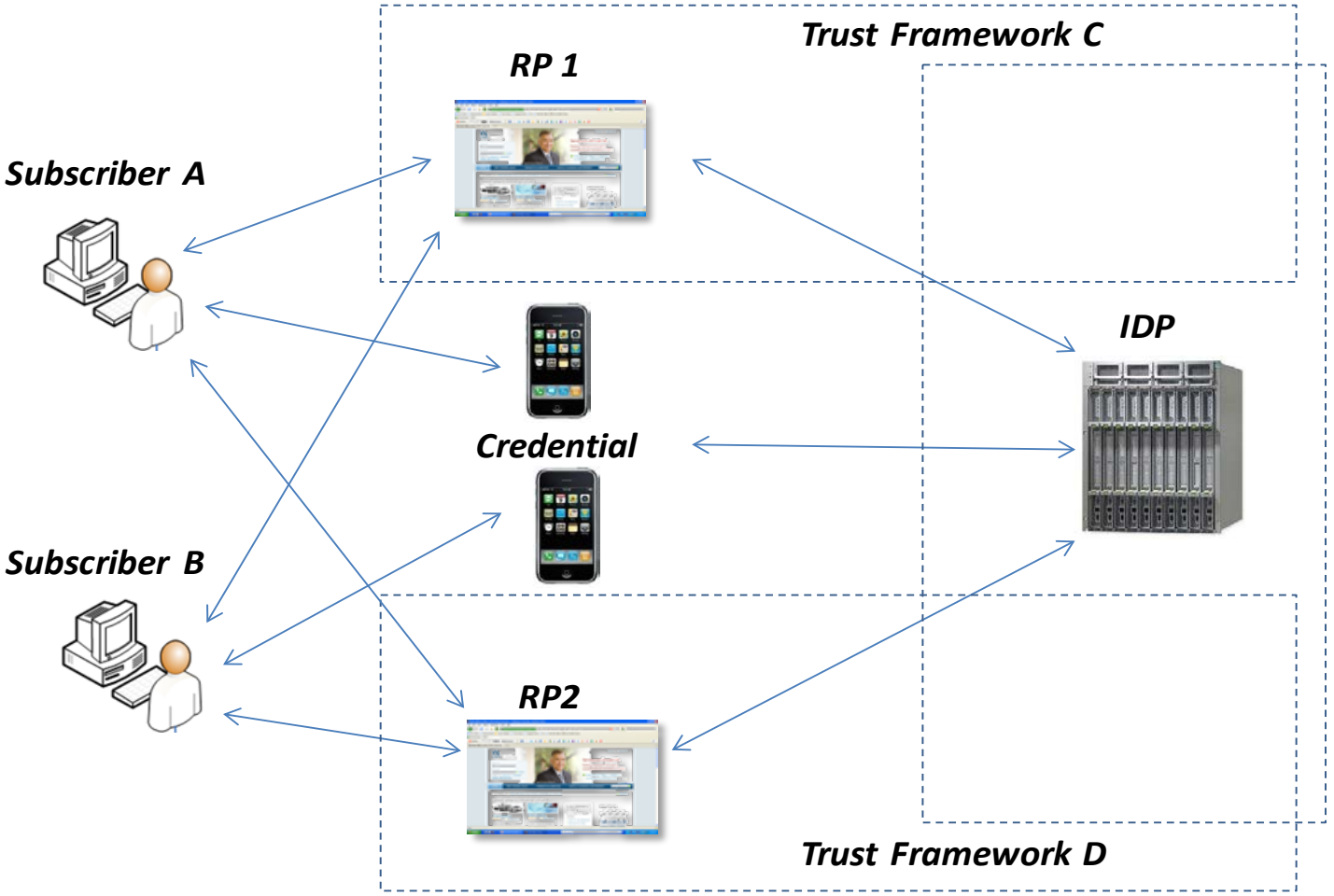


Addressing Guiding Principles

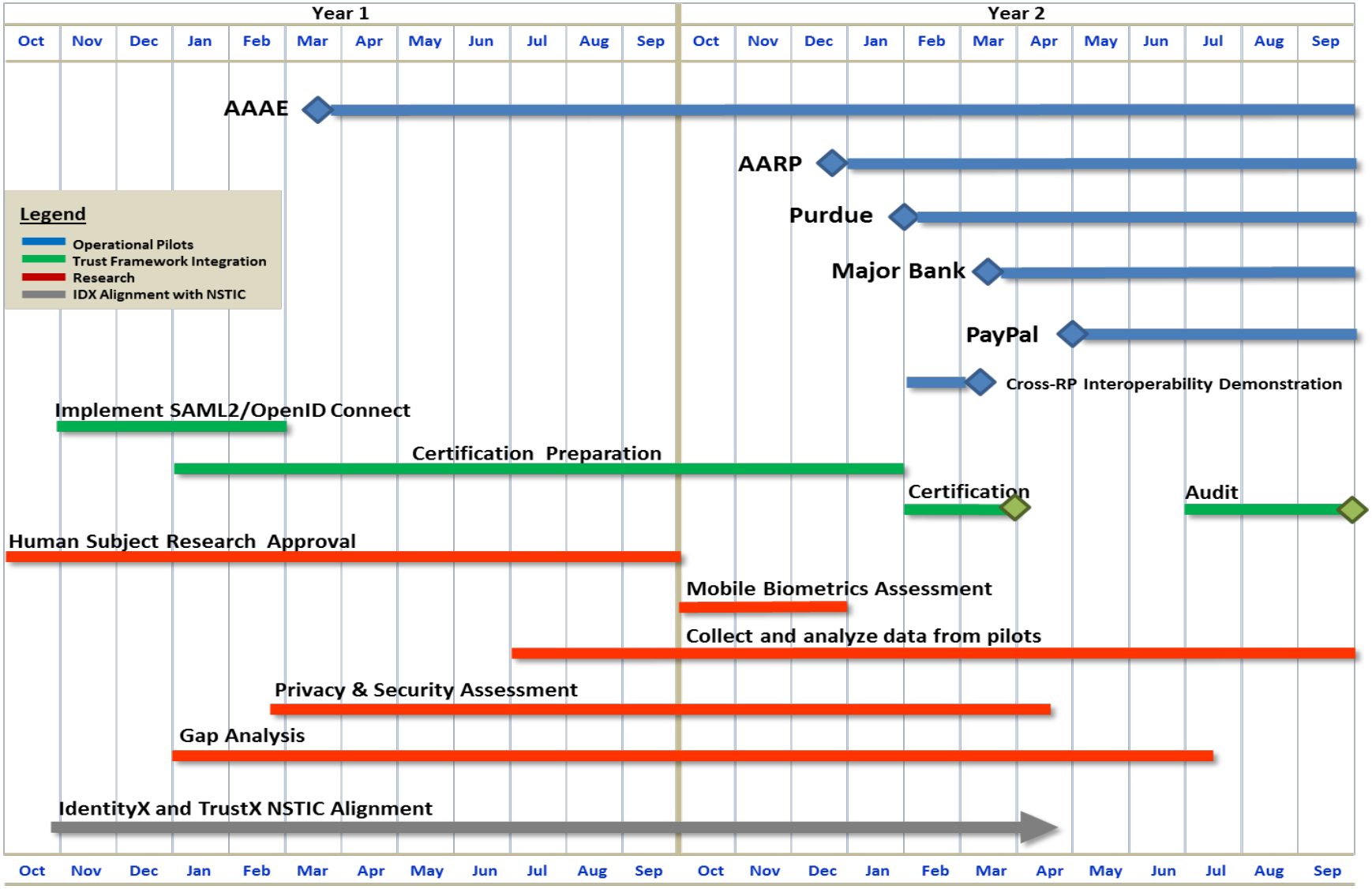
Daon

Principle	Affirm	Investigate/Enhance
Privacy enhancing & voluntary	• No PII stored on phone. • Authentication proportional to transaction risk level. • Opt-in pilots.	• Assess privacy • Investigate PETs
Secure & resilient	• Strong multifactor authentication • Server security assessment • High availability configuration	• Assess security, recommend improvements • Evaluate performance
Interoperable	• Supports multiple methods, hosted on multiple devices • Biometric independent	• Integrate with multiple trust frameworks • Demonstrate across multiple RPs
Cost effective & easy to use	• Use of existing mobile device is convenient and cost effective • RP/user choice of methods	• Assess usability, accessibility, and user acceptance

Interoperability Goal



Schedule



Proprietary and Confidential