NSTIC Pilots in the Wild –
The Daon Strong Authentication Pilot

C. Tilton
16 September 2014
Topics

• Background / Overview
• RP use cases
• RP business cases
• Demo (s)
Overview

What we are 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
Pilot at a glance

NSTIC & Trust Framework Standards

Gap Analysis

IDP

Operational Pilots

RP1

RP2

RP3

RP4

RP5

Subscribers

Data/Metrics

Data Collection & Analysis (inline)

Purdue Labs (offline)
What is TrustX?

• A 3rd party, hosted, multi-tenant identity service provider built around Daon’s IdentityX authentication platform.

• A component service – strong credential provider or “Token Manager”
  – Does not do identity proofing or storage of identity data
  – Privacy enhancing

• Can be used by an RP, IDP, or broker to provide strong, interoperable credentials
  – RP binds this credential to the subscriber account after proofing/authenticating

• RP controls authentication policy on transaction-by-transaction basis
What is different about us?

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

RIP

Passwords
Operational Pilots – Purdue University

- **PassPort** - Purdue IT-developed learning system that demonstrates academic achievement through customizable badges.
  - Integrates with Mozilla OpenBadges
  - Using this infrastructure, any organization can use, create, and issue badges

- Purdue has extended their existing Passport application to allow for multiple authentication options – e.g., FaceBook Connect
  - They have added TrustX as a high assurance option

- Authenticating via TrustX, students used to upload assignments and mid-term exams.
  - Higher confidence in who is submitting work
  - Spring 2014 completed, Fall 2014 in preparation
AARP is investigating ways to better protect their members – and their identities – when they are online.

Pilot goals:

- 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
Operational Pilots – AARP

- **AARP Health Record™** - an easy-to-use, online tool designed to help people over 50 manage their family health care needs.
  - This personal health record (PHR) allows members to safely store and access critical health information such as medications, allergies, blood type, immunizations and emergency and provider contact information.

- AARP is piloting the use of Daon’s TrustX™ strong, federated credentials to protect potentially sensitive health information.
  - They hope to learn how well this technology works with their demographic

- Phase I underway; Phase 2 tentatively scheduled for fall.
AAAE is a partner in the DTIS joint venture created to provide cost-effective and expedient background checking services.

DTIS provides background checking services for the aviation industry and the states of Alabama, Illinois, and Florida.

These services are made available onsite through ‘The UPS Stores’ 80+ locations.

Most background checks are performed for reasons of employment or volunteer work, frequently related to contact with vulnerable populations (children, elderly, disabled, etc.)

However, U.S. Department of Justice Order 556-73 allows US citizens to request a copy of their own FBI criminal history record for review – very much like requesting a copy of your credit report – as a means of double-checking what is contained in these records.
In the past individuals could request a copy of their FBI Criminal History Record Check:
• Fill out paper forms
• Visit local police for ink-card fingerprinting
• Submit forms and ink cards to FBI along with payment
• Wait for paper results via certified mail

Under FBI DO people now have an option for secure electronic submission and results
• Package submitted by a certified FBI CJIS Channeler (such as DTIS)
• Access to results online is limited to requesting individual who must be authenticated with strong MFA.

Current estimates are over 300K citizen-initiated requests for background check results annually (nationwide) under the old process.
Operational Pilots – AAAE/DTIS

- Why Double-Check?
  - Information in your CHR can affect your eligibility for many employment opportunities, may preclude you from certain benefits and may be cause to deny or revoke a security clearance.
  - Therefore - verify that you understand what is in your report BEFORE you apply for a job.
  - Avoid
    - Forgetting about something from years past
    - Discovering that something you thought was expunged - wasn’t
    - Discovering that the report lists an arrest but doesn’t show that you were acquitted, found innocent, or the charges dropped.
What is NSTIC-ie about this?

DTIS, acting as a relying party, will utilize Daon’s TrustX™ mobile device based multifactor authentication to protect this sensitive transaction.

Once receiving a TrustX credential it can be used at other RPs accepting these interoperable credentials.

Goal is to build the subscriber base while providing a useful commercial/consumer service that people are willing to pay for

Set to launch this fall
Impacts on RPs

- Stronger authentication options mean they can conduct higher risk transactions online
  - Can select methods dynamically, totally under RP control
    - Flexibility
    - Trust elevation (step-up authentication)
  - Can accommodate user preferences and capabilities

- Biometrics seen as a means of increasing user convenience
  - Not just security

- Another choice in the federated identity marketplace
  - Multifactor ≠ Password + SMS/OTP