



# Daon TrustX Pilot

*C. Tilton*

3 December 2013



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.



# Who is TrustX?



- TrustX is a wholly owned subsidiary of IdentityX
  - So ... what is IdentityX?
- IdentityX is a Daon company
  - And who the heck is Daon?
- Daon is best known for our large scale biometric identity systems:
  - National ID systems – Mexico, India, Portugal, Qatar
  - Border management systems – EU, Japan, Australia, NZ, US
  - Biometric enrollment and background screening services





## Advancing Commercial Participation in the NSTIC Ecosystem





# 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



# Our Pilot Elements



Technology

Operational Pilots



Research

Trust Frameworks





# Identity **X** is ...

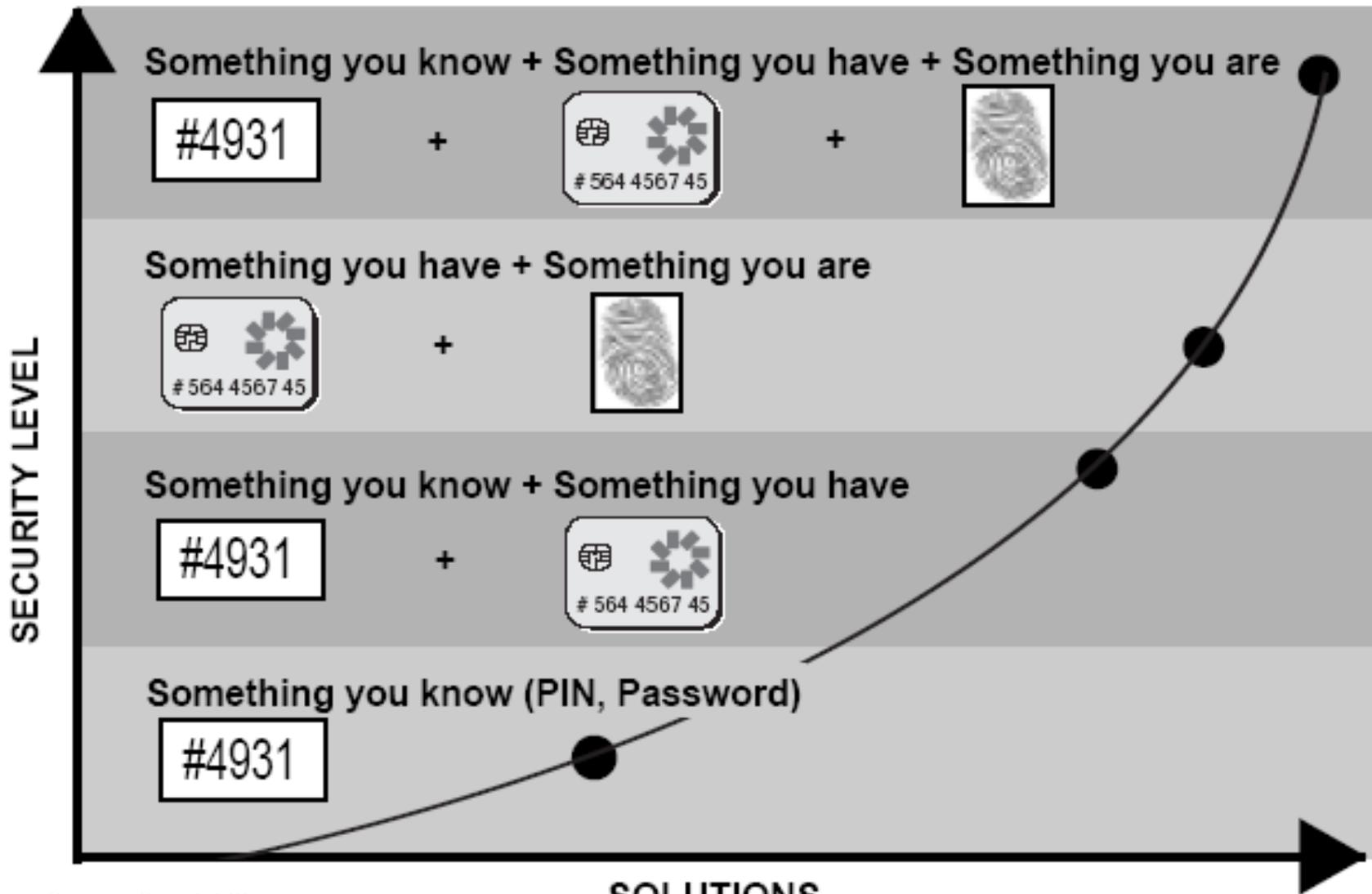


- A unique risk-based, multi-factor authentication capability that leverages latest generation smart phones (e.g., iPhone, Blackberry, Android), smart tablets (e.g., iPad/Playbook) and traditional mobile devices
- Identity **X** technology combines multiple authentication techniques for greatest identity 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 consumers
- Designed to run both as an in-app framework and out-of-band authentication product





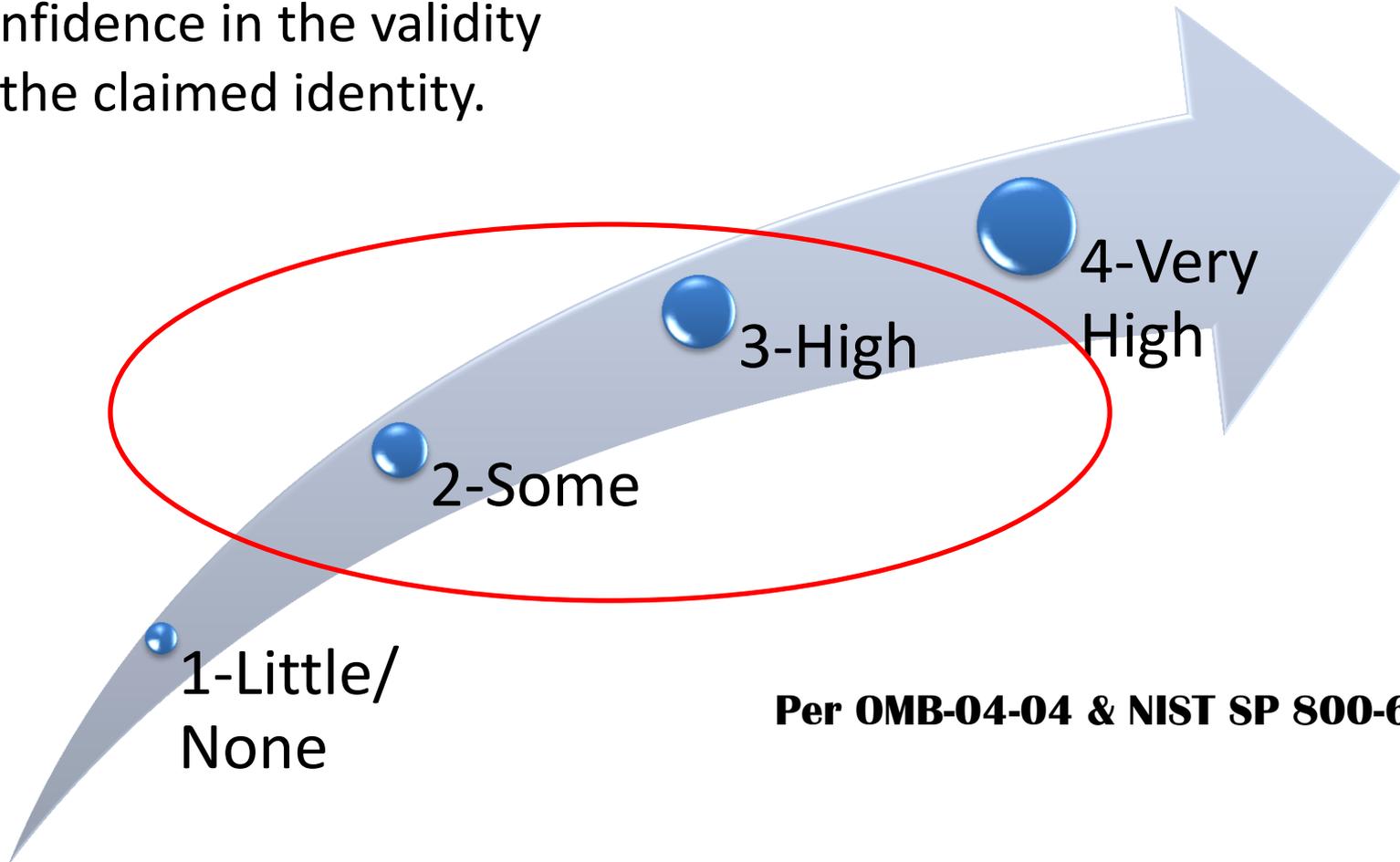
# Multifactor Authentication





# Assurance Levels

Confidence in the validity of the claimed identity.



**Per OMB-04-04 & NIST SP 800-63**



# Token Types

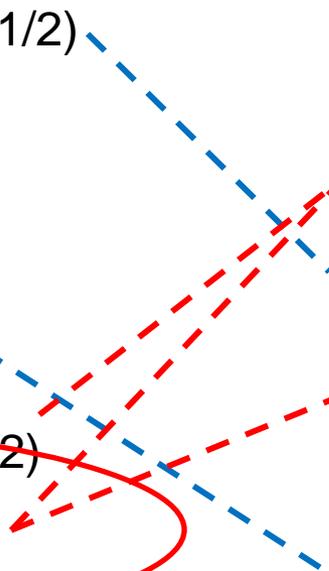


## 800-63-1 Token Types

- Memorized secret token (L1/2)
- Pre-registered knowledge token (L1/2)
- Look-up secret token (L2)
- Out of band token (L2)
- SF OTP device (L2)
- SF cryptographic device (L2)
- MF software cryptographic device (L3)
- MF OTP device (L4)
- MF cryptographic device (L4)

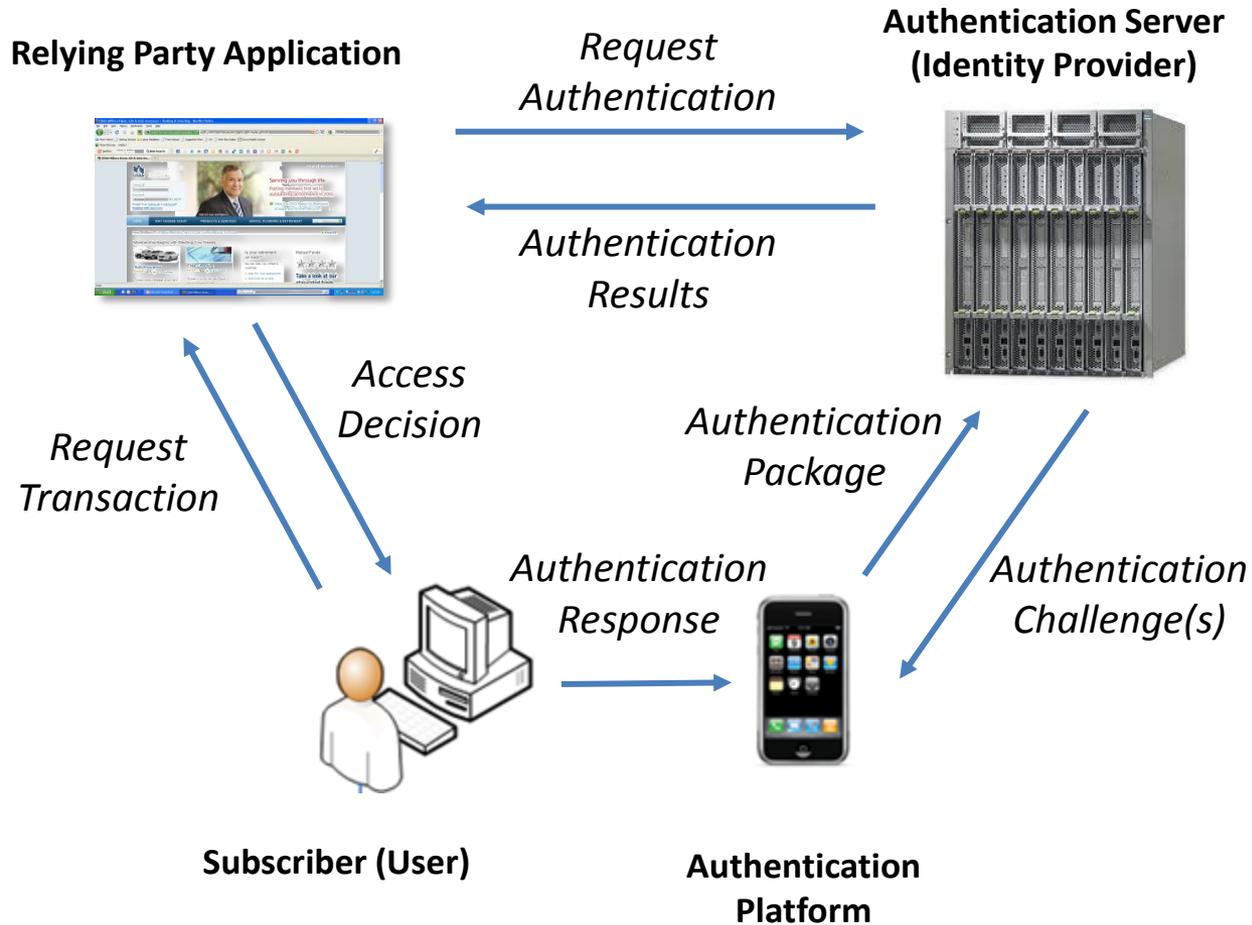
## IdentityX Token Types

- Possession of phone (device ID)
- Possession of phone (soft cert)
- PIN
- Face (basic/liveness)
- Voice (basic/liveness)
- [Palm]
- OOB OTP
- Geolocation





# Technology - Identity X





# TrustX is ...



- An Identity Provider (IDP) for delivering highly secure authentication services to businesses and consumers
- A multi-tenant service hosting multiple applications from different Relying Parties
- Based on IdentityX authentication.





# 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 – “full IDP” and “CSP only” support
- Supporting multiple RP interfaces – SAML2 & OpenID Connect





## Credential Service

- Strong credential issuance, mgmt, 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

## Identity Provider Service

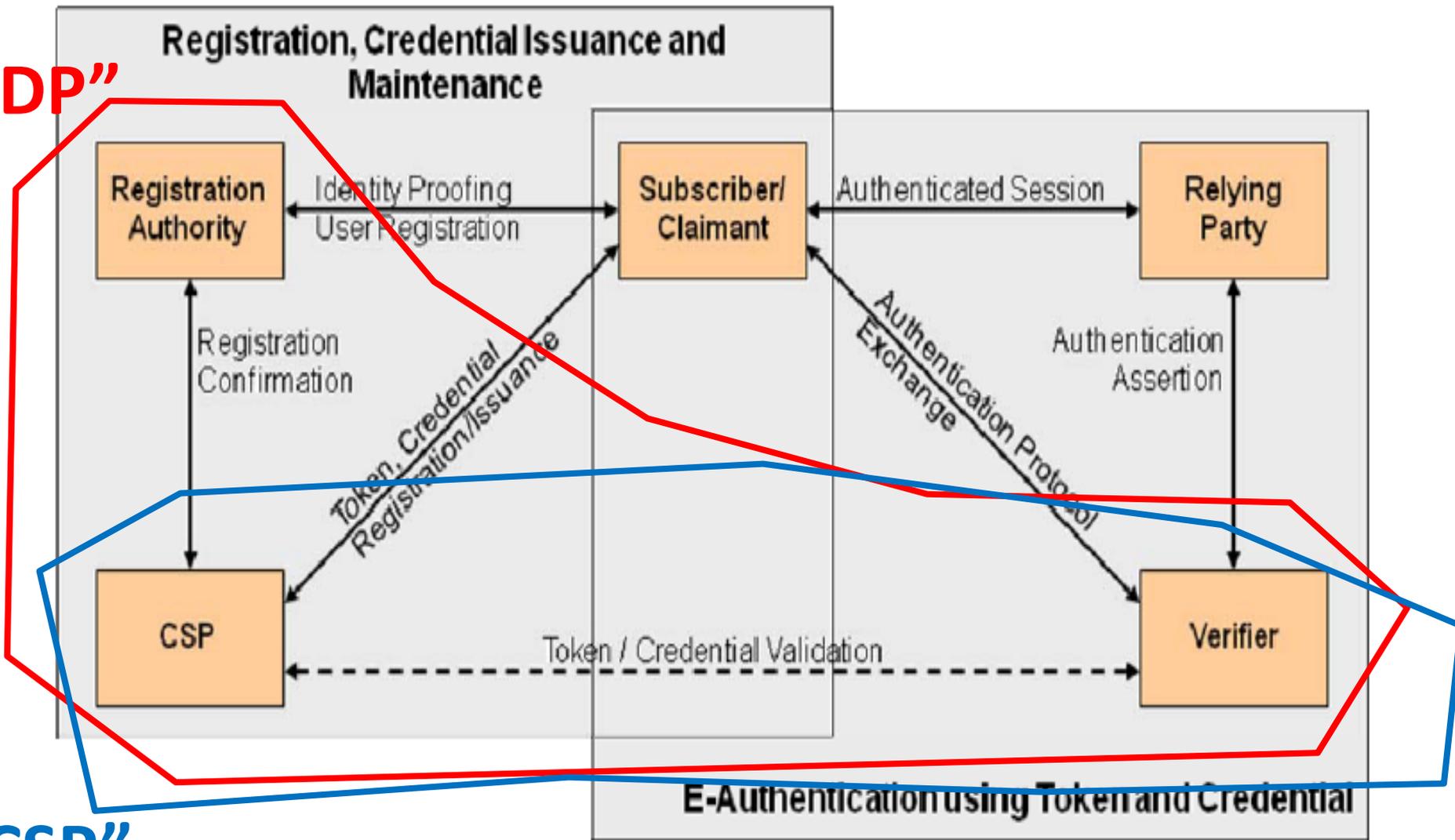
- Full IDP service:
  - Identity proofing (via partner)
  - Hold min set of data
  - Credentialing also
- Single credential can be bound by multiple RPs
- Support subscriber approved sharing of identity data
- LOA3 for all



# SP800-63 Model



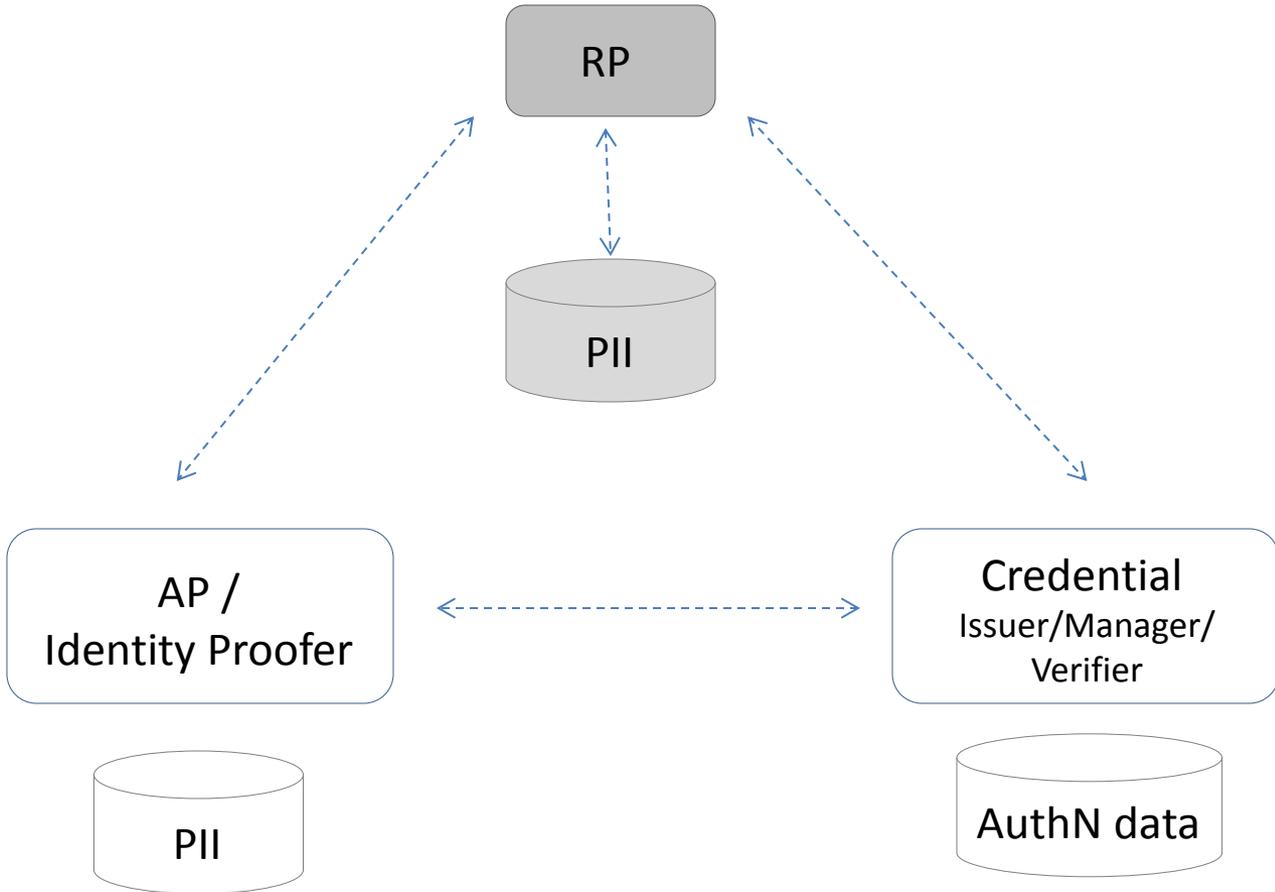
**“IDP”**



**“CSP”**

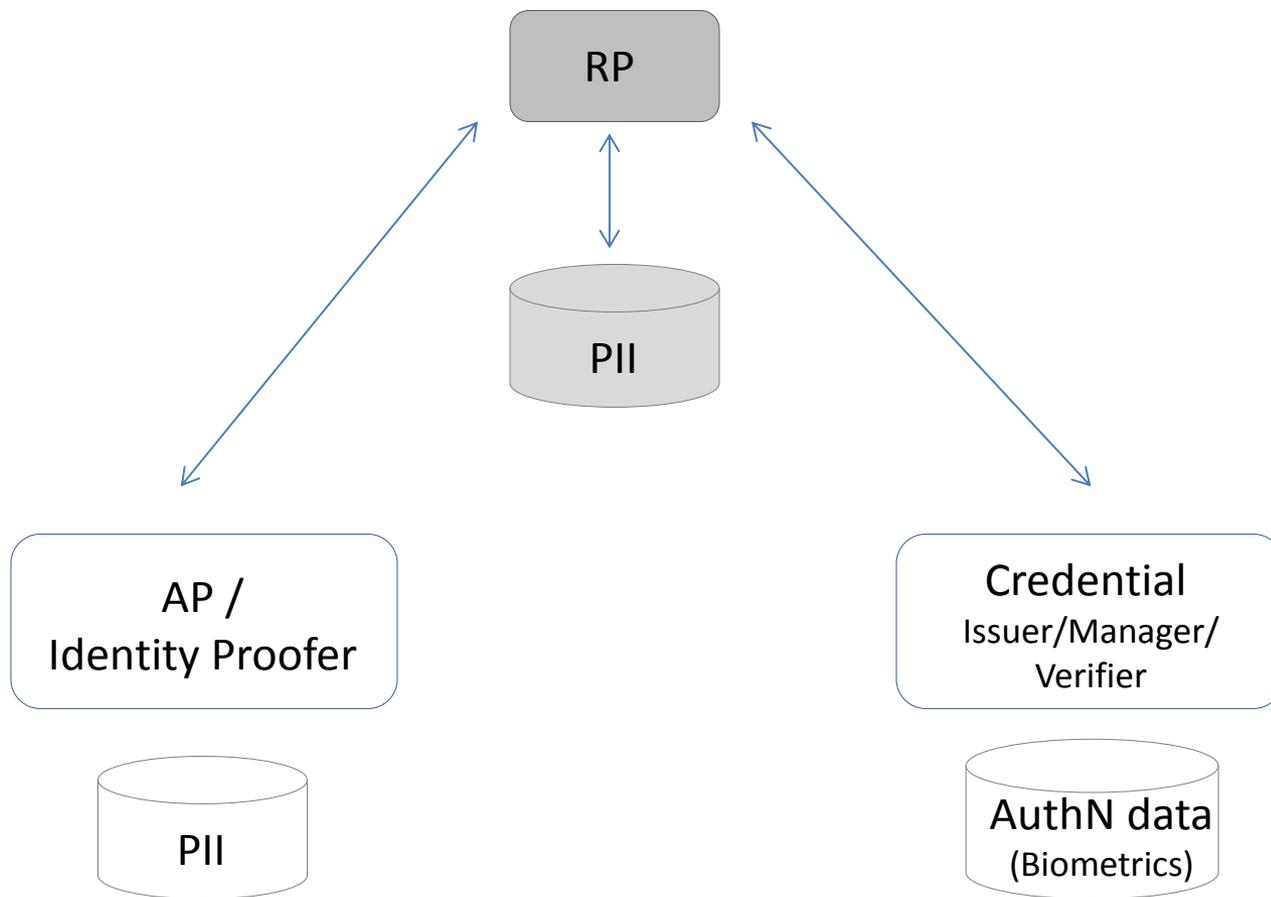


# Services



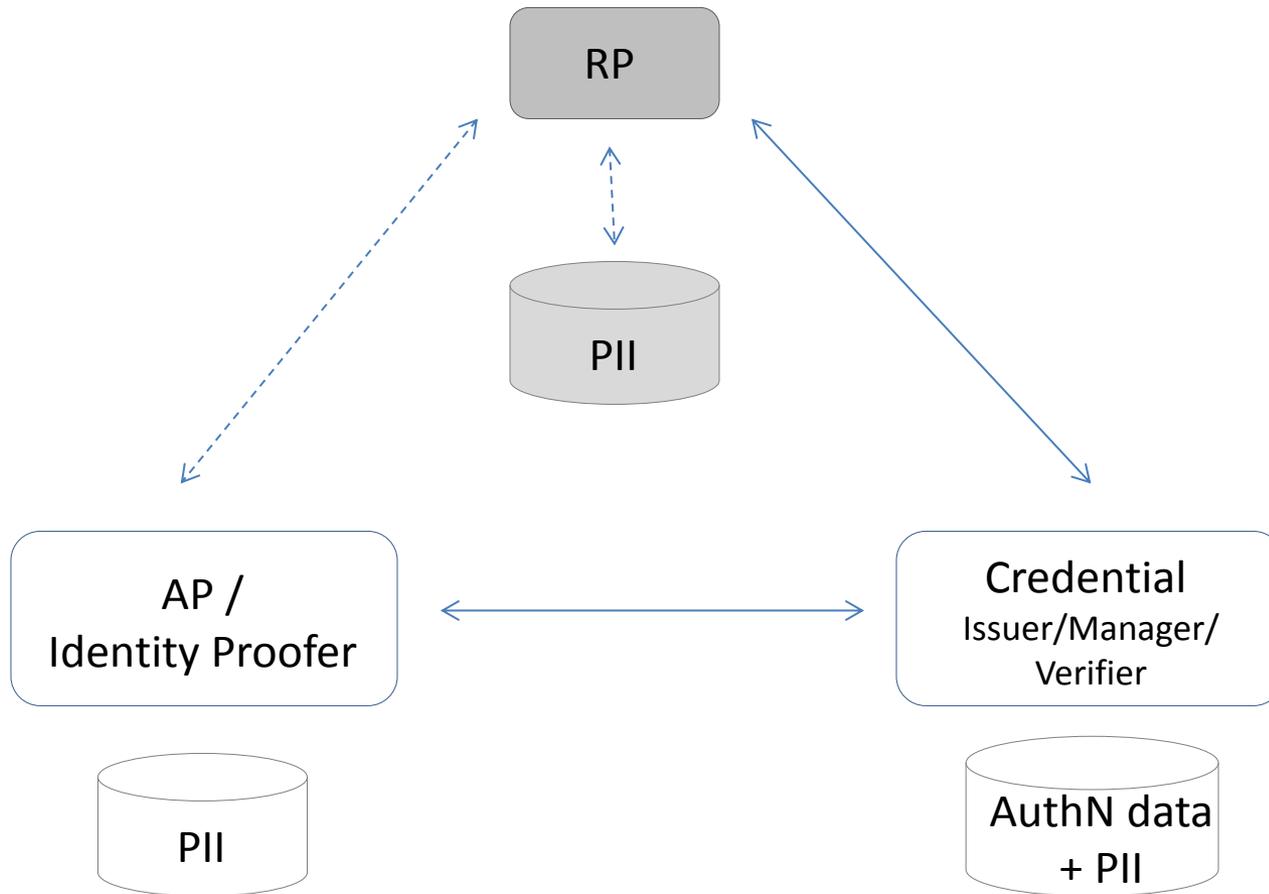


# CSP Service





# IDP Service





# Trust Frameworks – NSTIC Alignment



InCommon®

SAFE-BioPharma.



- 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

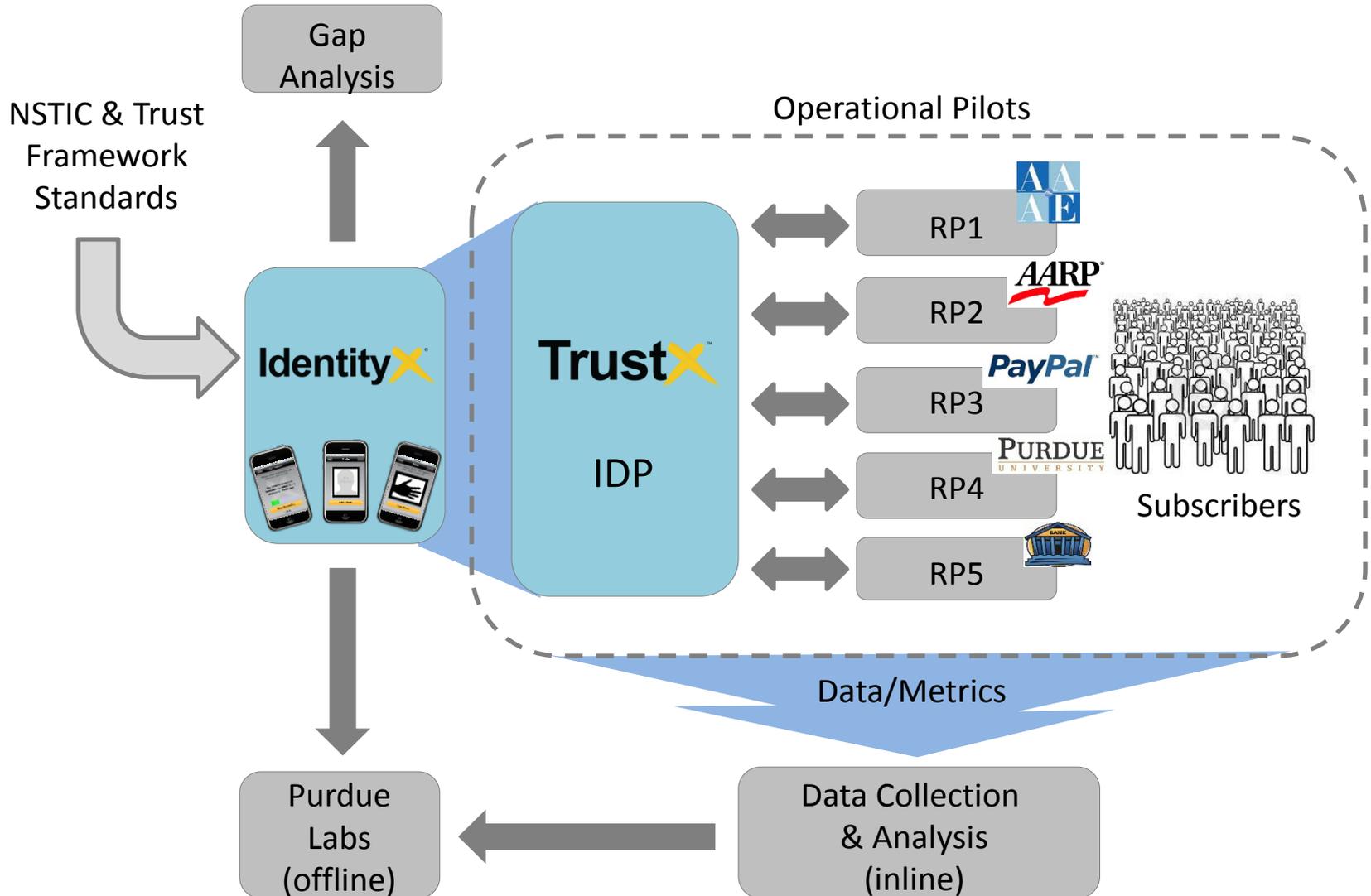


- Biometric Standards, Performance & Assurance Laboratory (BSPA)
- Center for Education and Research in Information Assurance and Security (CERIAS)
- Practical research
  - Offline - Laboratory
  - Online – Analyzing data from the operational pilots
- Areas
  - Usability
  - Accessibility
  - Privacy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





# Operational Pilots





# 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



## ■ 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 3<sup>rd</sup> 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



# Use cases



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	Premium Services	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

# Demonstration

---



# Demonstration



Video



# Link to Video

<http://www.youtube.com/watch?v=hOj0PvL234M>



# 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 Member

Membership is as little as \$1 a month!

**AARP**  
Real Possibilities

Please log in or register in order to subscribe to newsletters, create a profile, comment on articles, and so much more!

Email Address:

OR

Log in using your existing social account:

Facebook Twitter Google+ LinkedIn YouTube AOL

Forgot your password?

**LOG IN**

**Why Register with AARP.org?**

- Play online games and save your top scores
- Subscribe to our Daily News Alert, Webletter, discount alerts, topical newsletters, local event updates and lots more
- Store your photos and share them with friends and family
- As an AARP member, register to manage your membership account online and enjoy exclusive content and benefits

**REGISTER**

Website Access/Login



Portal

Premium Services



Data vaults

Individual Services



Level of Authentication



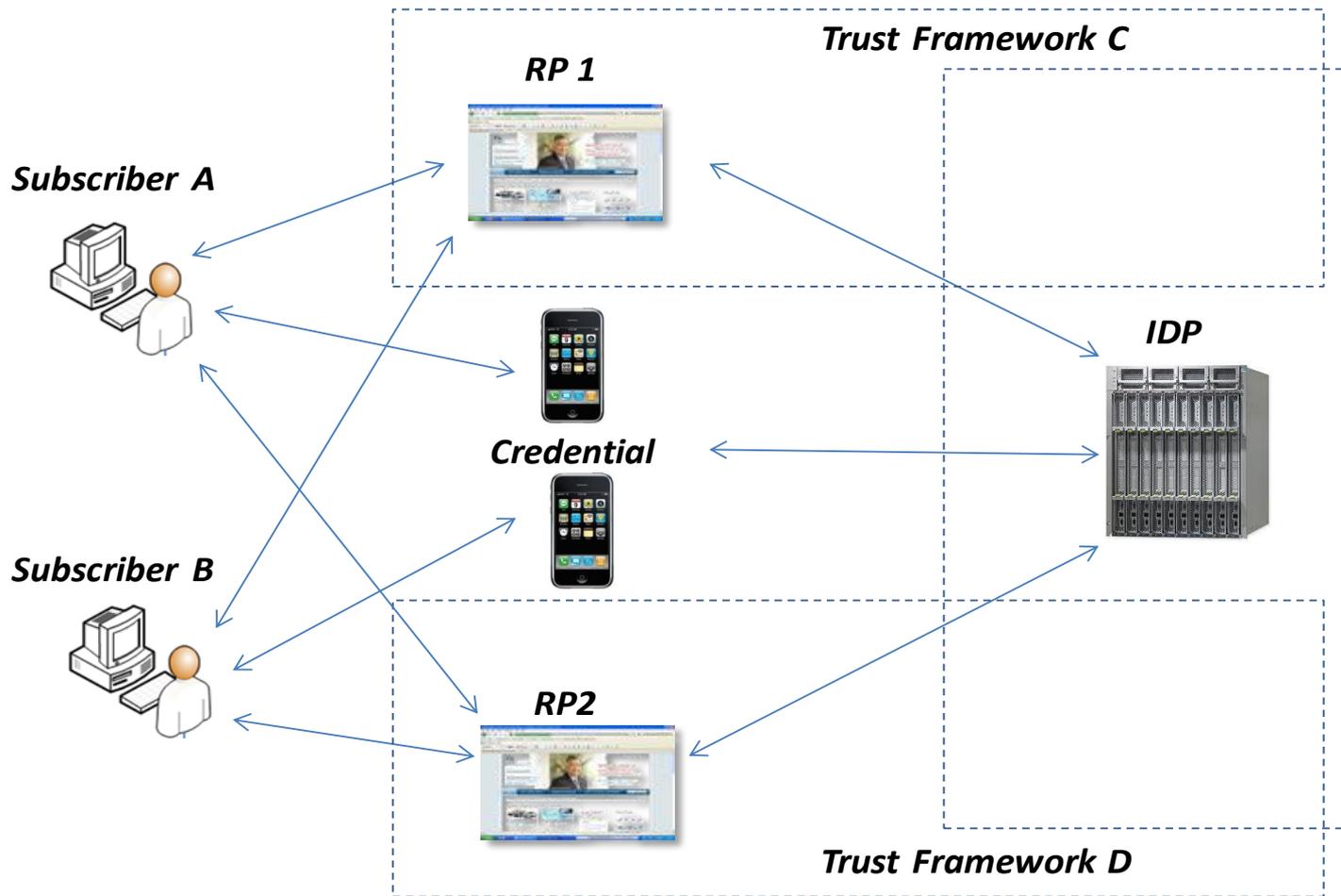
# Addressing Guiding Principles

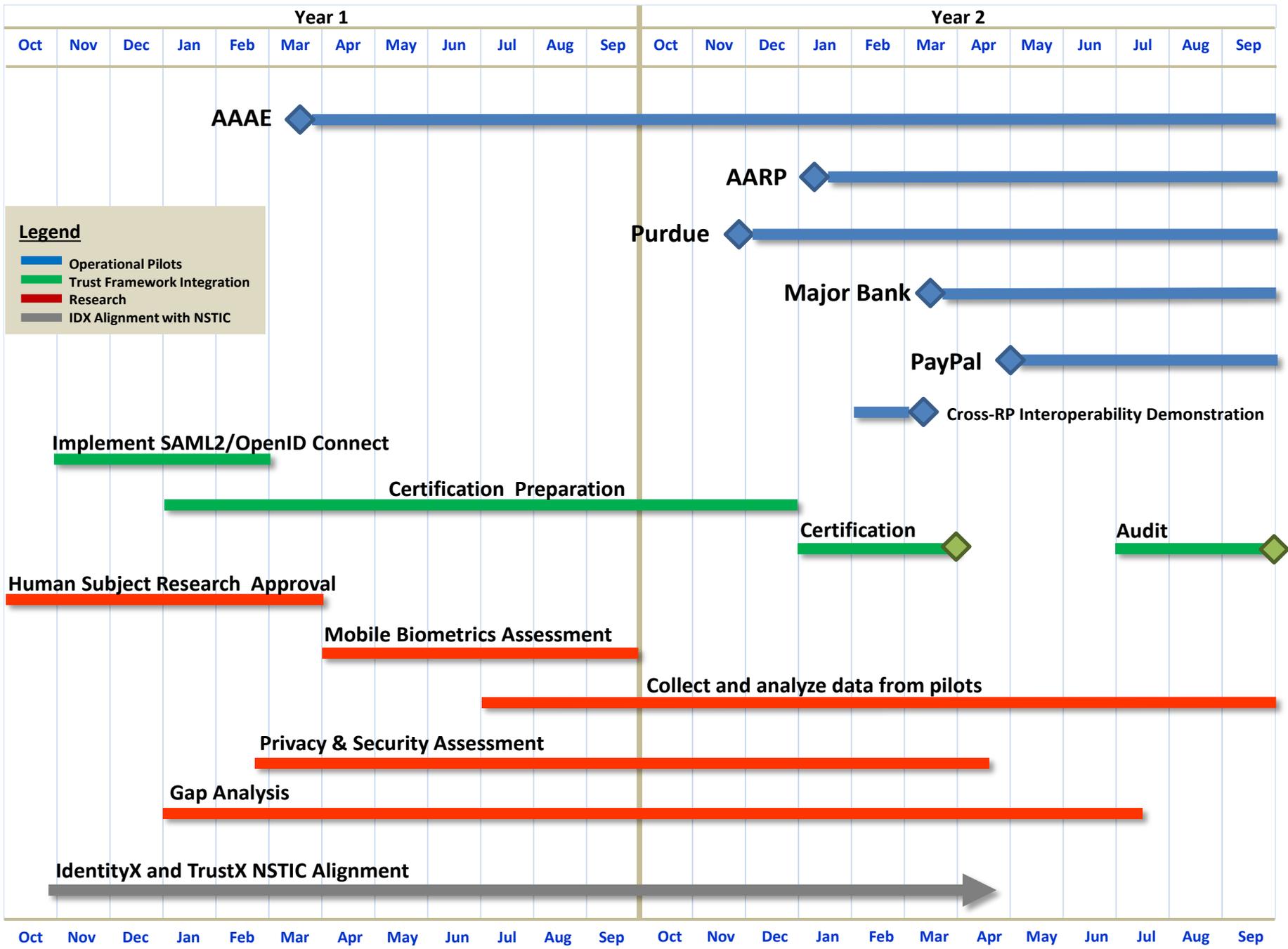


Principle	Affirm	Investigate/Enhance
Privacy enhancing & voluntary	<ul style="list-style-type: none"> <li>No PII stored on phone.</li> <li>Authentication proportional to transaction risk level.</li> <li>Opt-in pilots.</li> </ul>	<ul style="list-style-type: none"> <li>Assess privacy</li> <li>Investigate PETs</li> </ul>
Secure & resilient	<ul style="list-style-type: none"> <li>Strong multifactor authentication</li> <li>Server security assessment</li> <li>High availability configuration</li> </ul>	<ul style="list-style-type: none"> <li>Assess security, recommend improvements</li> <li>Evaluate performance</li> </ul>
Interoperable	<ul style="list-style-type: none"> <li>Supports multiple methods, hosted on multiple devices</li> <li>Biometric independent</li> </ul>	<ul style="list-style-type: none"> <li>Integrate with multiple trust frameworks</li> <li>Demonstrate across multiple RPs</li> </ul>
Cost effective & easy to use	<ul style="list-style-type: none"> <li>Use of existing mobile device is convenient and cost effective</li> <li>RP/user choice of methods</li> </ul>	<ul style="list-style-type: none"> <li>Assess usability, accessibility, and user acceptance</li> </ul>



# Interoperability Goal







## Learn More



- Daon Pilot POC:
  - Cathy Tilton, [cathy.tilton@daon.com](mailto:cathy.tilton@daon.com), 703-472-5546
  
- Interested Relying Parties
  - Jim Williams, [jim.williams@daon.com](mailto:jim.williams@daon.com), 202-465-5150
  
- TrustX & IdentityX websites
  - [www.trustx.com](http://www.trustx.com)
  - [www.identityx.com](http://www.identityx.com)
  
- NSTIC
  - [www.nist.gov/nstic](http://www.nist.gov/nstic)
  
- IDESG
  - [www.identityecosystem.org](http://www.identityecosystem.org)