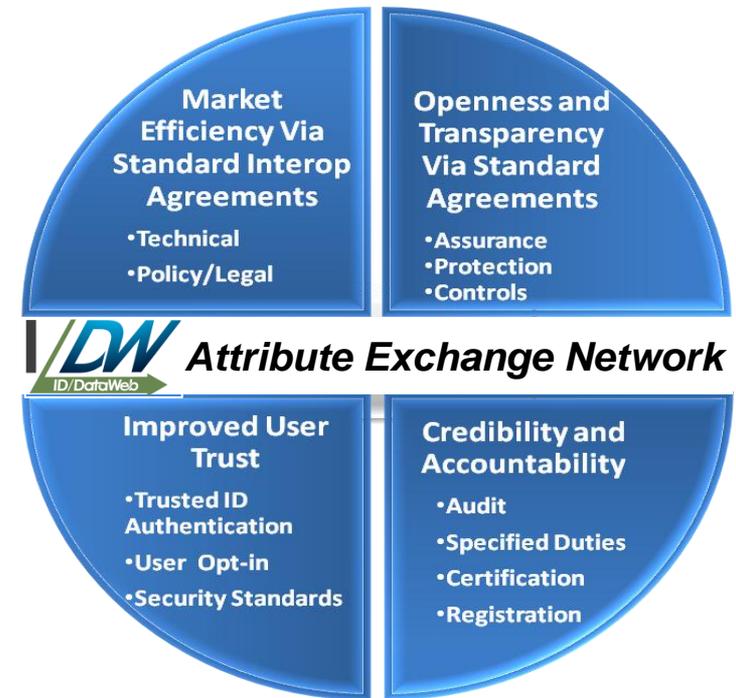




***Online Identity Attribute Exchange
2013 - 2014 Initiatives***

Agenda

- Overview
- AXN Services Framework
- Demonstration
- NSTIC Pilots
- Summary
- ABAC Services





AXN - Enabling IT & Other Values

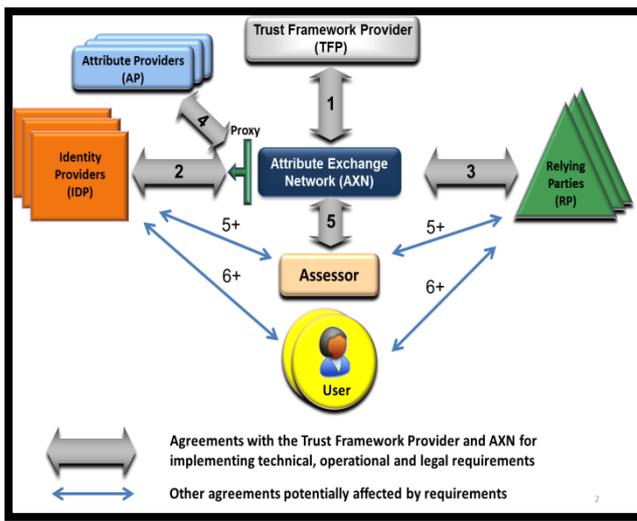
- Web SSO using a known login
 - **Credential Federation** – *verified attributes are used to create new or bind to existing user accounts*
 - Reduces drop off, account creation and maintenance costs
- Federated IDaaS – cloud transaction hub
 - Real-time commercial & authoritative attribute verification
 - IdP credential authentication federation (LOA 1 – 4) plus contextual trust elevation methods for sensitive transactions
- **Neutral** credential and attribute marketplace
 - Efficient, open, competitive exchange – best of breed and value
 - Free to users; lowers RP costs; a new channel for IdPs and APs
- Contractual and policy management hub
 - One RP contract to access competitive AP and IdP services
 - Standard agreements with flow down terms from IdPs and APs
- Privacy by design
 - User opt-in, User Management Console, and data minimization
 - AXN is a transaction proxy with no central data store of Pii

NSTIC Guiding Principles

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

OIX AX Trust Framework

- Credential & Attribute Exchange
- Business, Legal, Technical, Privacy, Audit/Certification
- Industry Driven



Contractual & Policy Control Points

Federated Identity Use Cases



- **Federated Consumer Login** - user credential of choice to create accounts (using verified, user-asserted attributes) and to enable SSO
- **Business Process Outsource Services** – community hubs for outsourced transaction services
- **Enterprise Attribute Based Attribute Control (ABAC)** – federated login using verified attributes for policy-controlled access to shared resources
 - Mitigate data leakage to control service, application and data level access
 - Managing content providers, content, and real-time distribution
- **Supply/Value Chain**– federated login (using many IdP credentials) to enterprise resources for employees, partners, and consumers
 - Rationalizing credentials for federated login
 - ABAC driven access to shared resources
- **New Federation Applications** – enhanced access, mobility, usability, and collaboration

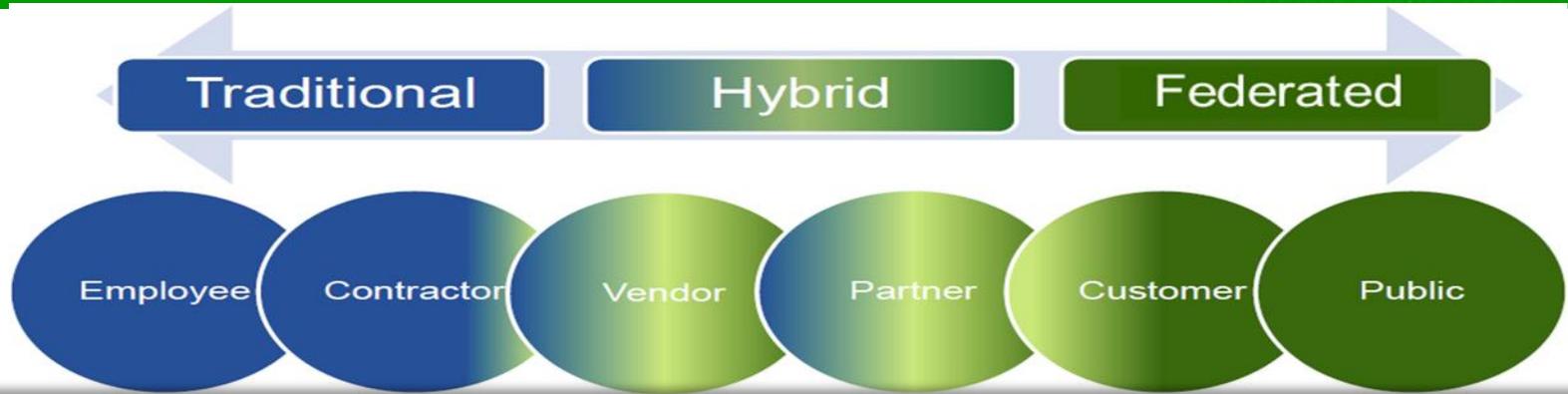


The First Year NSTIC Use Cases



		Industry
	Broadridge Use Case RP Service: Fluent – Online Application Platform for Investor Communications	B to C Investor Communications
		Industrial Enterprise Use Case (Pending Final Approval) RP Service: Various Service Sector Applications Corporate, Partner and Consumer Account Access
	DHS/FEMA (MIT Lincoln Labs) First Responder Use Case RP Service: Account creation and login for the First USA disaster response collaboration portal	G to G, G to C First Responders First USA Services
		eBay Use Case RP Service: Retail Seller and Buyer Account Creation and Login

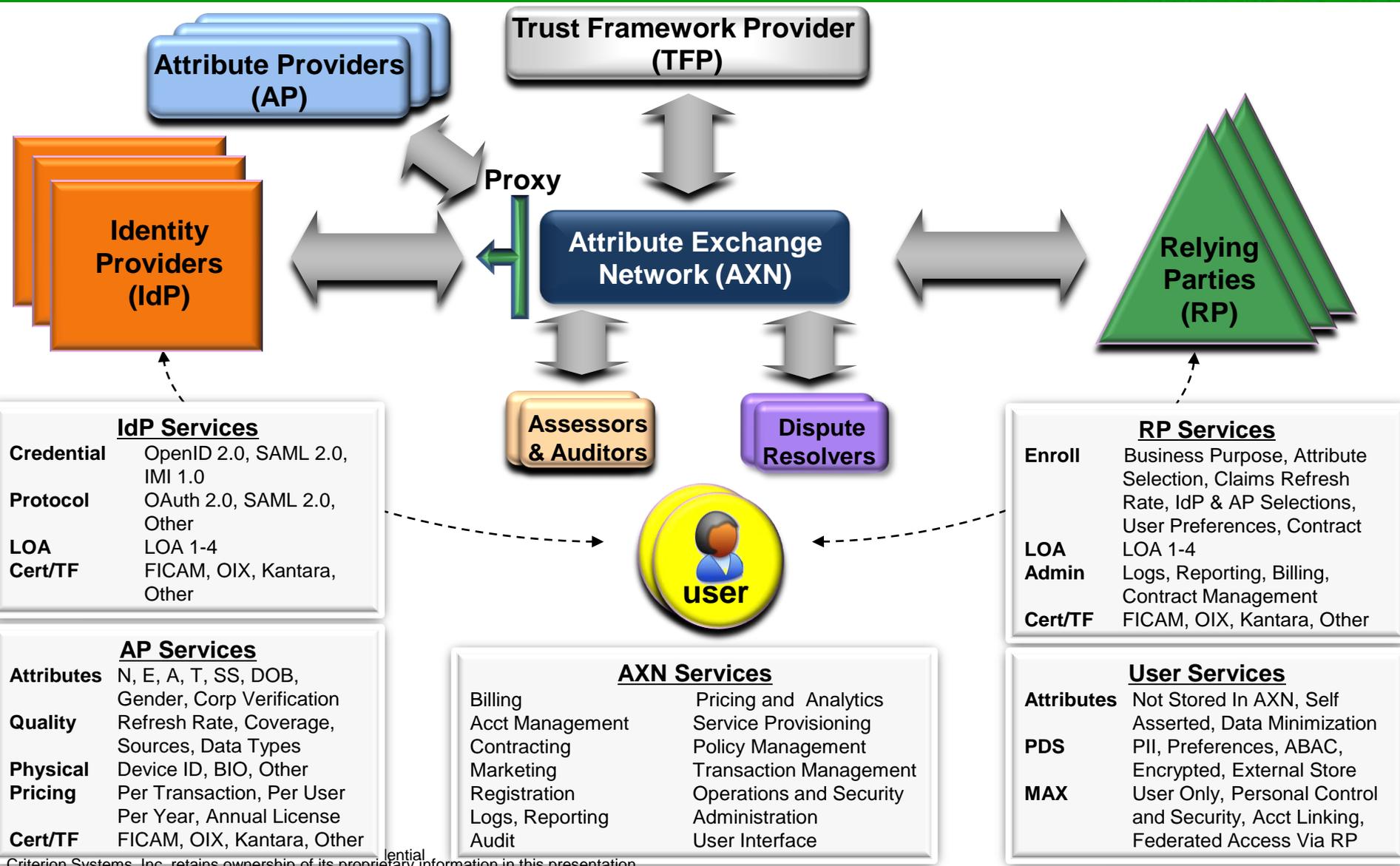
IdAM Constituency To Approach



Source:
Gartner Group

Life Cycle/ Constituency	Employee Services	Contractor Services	Vendor Services	Partner Services	Customer Services	Public Services
Purpose/Posture	Enable/Provide/ Manage/Collect	Enable/Provide/ Manage/ Collect	Enable/Manage/ Collect	Enable/Provide/ Support	Expose/Sell/ Service/Provide	Expose/Sell/ Service/Provide
Life Cycle Event / Options	Ent. Admin/ Change in Authoritative Source	Delegated Admin/Change in Authoritative or Federated Source	Delegated Admin/ Self- service/Federated Provisioning -SCIM	Delegated Admin/ Self- service/Federated Provisioning -SCIM	Self Service/ Social Identity (OpenID)/ Federated Provisioning -SCIM	Self Service/ Social Identity (OpenID)/ Federated Provisioning -SCIM
ID Store	Enterprise Directory	Federated Enterprise Directory	Federated Enterprise Directory/ VDS	Federated Enterprise Directory/ VDS	Federated Enterprise Directory/ VDS	Federated Enterprise Directory/ VDS
Authorization	Roles/Rules/ ABAC	Sponsored Roles/Rules/ ABAC	Roles/Rules/ ABAC /OAuth or SAML	Roles/Rules/ ABAC /OAuth or SAML	Roles/Rules/ ABAC /OAuth or SAML	Roles/Rules/ ABAC /OAuth or SAML
Authentication	Username/Pswd/ Strong Auth/ Federate/ID Proofing	Username/Pswd/ Strong Auth/ Federate/ Adaptive Access/ID Proofing	Username/Pswd/ Strong Auth/ Federate/ Adaptive Access/ID Proofing			
Audit	Access Cert./Reporting	Access Cert./Reporting	Access Cert./ Reporting/ Real- time Monitoring	Real-time Monitoring/ Fraud Detection	Real-time Monitoring/ Fraud Detection	Real-time Monitoring/ Fraud Detection

AXN Services Framework





AXN Trust Elevation Services

Device Attribute Verification Services

- Mobile Device Verification Services
 - Users log in using a trusted mobile device registered and managed on the AXN via MAX
 - Secure device ID service ensures user RP accounts can only be accessed using a trusted device
- Computer Verification Services
 - Over 600 million computers with Trusted Platform Modules (TPMs) can be managed via the AXN
 - Windows 8 requires TPMs on a wide range of devices from desktops to smart phones

Biometric Attribute Verification Services

- Cloud-based Voice, Irisl, Photo and Fingerprint Verification Services
 - Daon, CGI, and others
- Integration with Authoritative AP Services
 - e.g., driver license attributes and photos

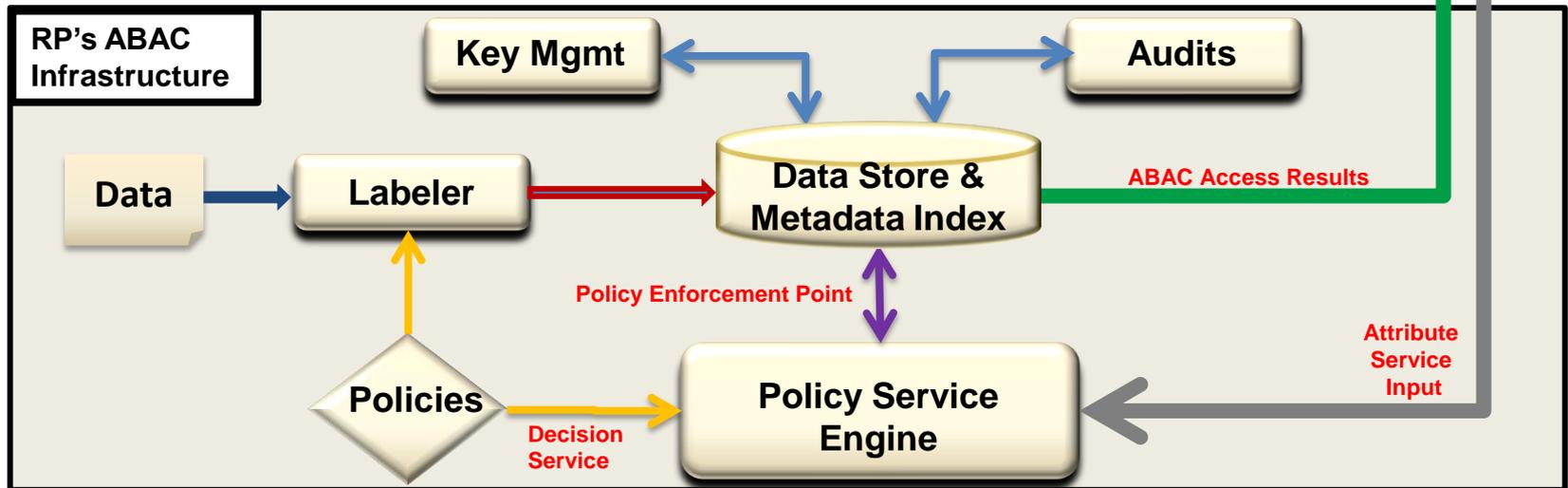
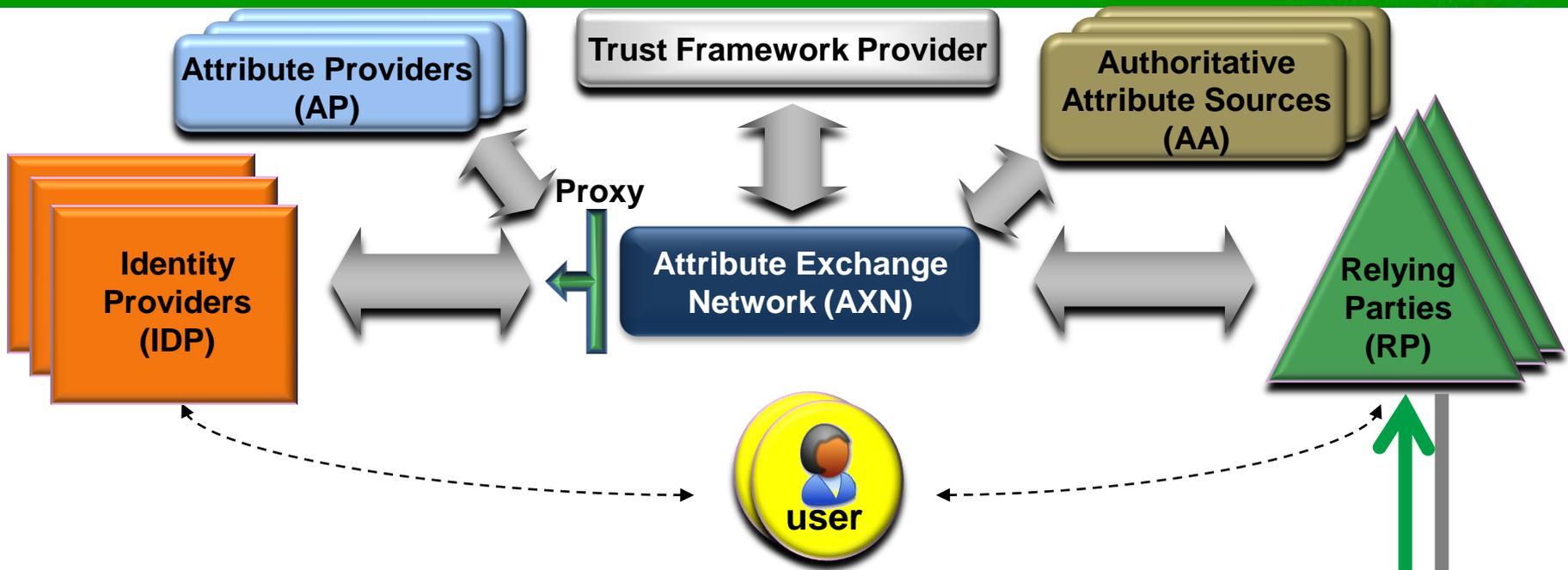
ABAC Services

- Fine-grained Policy Authorization Services
- UMA Services to Dynamically Control Access to RP Data and Services

	Verified Attribute Claim	AXN Trustmark Services			
		TMI	TM2	TM3	TM4
Low	PII	Name+ Email+ Address+ Telephone (NEAT)	TMI + DOB	TM2 + SSN4	TM3 + SSN9
↓ Cost	Device	PII+ SMS PIN + IPSEC	TMI + Device	TM2 + MDM	TM3 + GEO
	Biometric	None	PII + Device + Voice (Bio1)	TM2 + Bio2	TM3 + Bio3
	PKI Credentials	None	None	PII+ Device + PKI	TM3 + Biometric
Higher		Low	→ Cost →		Higher

Criterion-FCCX-03

AXN - ABAC Ecosystem



AXN Demonstration



Lessons Learned

- RPs are the customer, and will drive market requirements, adoption, and policy controls
- Emerging Trust Frameworks are being driven by Communities of Interest (COI) who seek market operational efficiencies through business, legal, technical and policy interoperability
- Credential federation requires policy changes to enable significant security, user experience (SSO and account creation), and business benefits
- Implementing Contractual Agreements can be iterative and time consuming
 - Start early; inform and engage key stakeholders
- A rigorous Privacy Evaluation Methodology (PEM) implementation resulted in significant benefits
 - Current IdP and RP business practices don't always conform to FIPP's, and can be managed
 - AXN technical and architectural enhancements
 - Privacy protective enhancements as core messaging in AXN marketing strategy
- RP risk mitigation strategies (for a required LOA) lack consistency
 - Emerging user-centric trust elevation technologies are scalable, cost effective and interoperable
 - Trust Marks could be used to objectively promote confidence in various combinations of authentication methods, verified user attributes, and attribute claims from device identities, biometric technologies, etc.
 - It would be helpful to map these risk mitigation methods to NIST SP 800-63



Summary



- 2013 - 2014 AX initiatives will demonstrate how to...
 - Improve User online experience, increase User trust and transaction volumes, and reduce related costs
 - Protect and extend customer relationships online
 - Manage organizational risks with cost effective solutions
 - Reduce online fraud and identity theft while enhancing brand
- Neutral market platform for identity credential federation and attribute exchange
- Online attribute monetization platform – unencumbered by legacy business models, regulations and technologies

