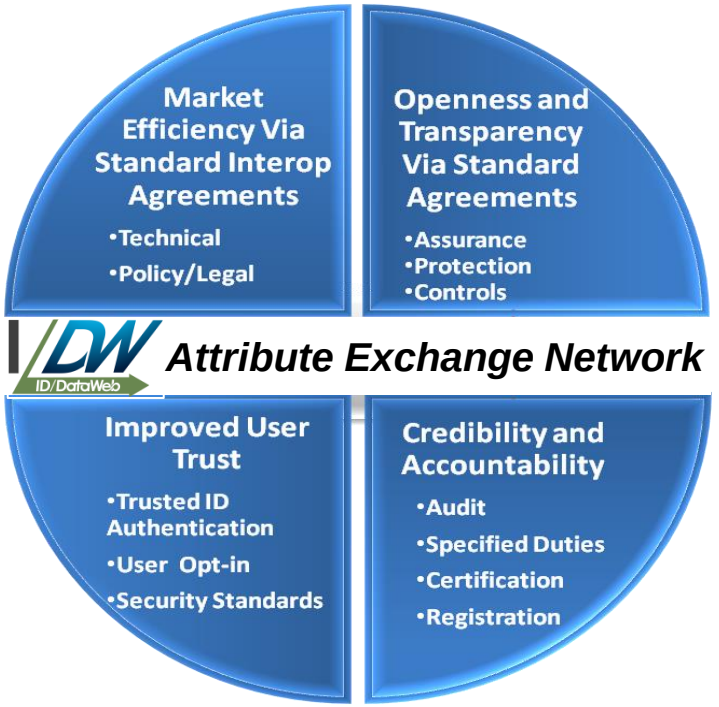
Online Identity Attribute Exchange
2013 - 2014 Initiatives

Agenda

- Trust Economics
- Trust Frameworks
- AXN Services Framework
- Trust Framework Implementation Tasks
- Lessons Learned
- Next Steps



Mission

Implement a global ecosystem where:

- ***individuals*** easily conduct trusted, privacy-sustaining, digital transactions
- ***organizations*** strategically benefit from interoperable, secure and cost competitive transactions
- ***service providers and others*** drive revenues in an open, efficient, large marketplace

… and everyone wins!

AXN - Enabling IT & Other Values

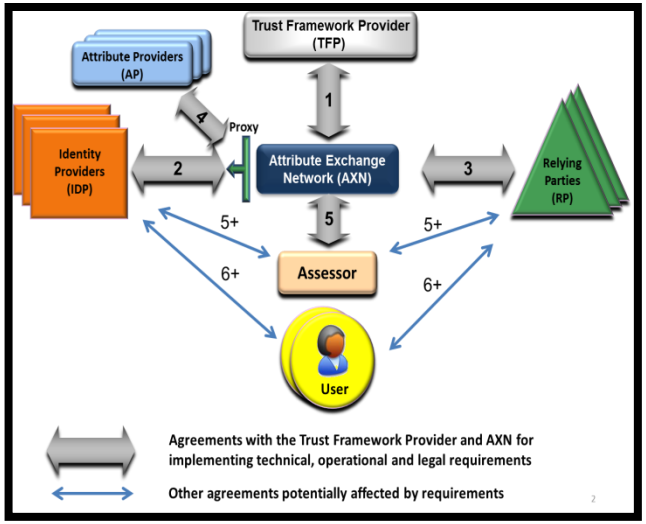
- Web SSO using a known login
  - ***Credential Federation –verified attributes are used to <u>create new or bind to existing</u> user accounts***
  - Reduces drop off, account creation and maintenance costs
- Federated IDaaS – cloud transaction hub
  - Real-time commercial & authoritative attribute 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

<u>NSTIC Guiding Principles</u>

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

<u>OIX AX Trust Framework</u>

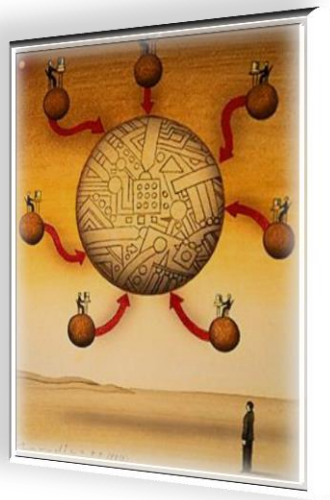
- Credential & Attribute Exchange
- Business, Legal, Technical, Privacy, Audit/Certification
- Industry Driven



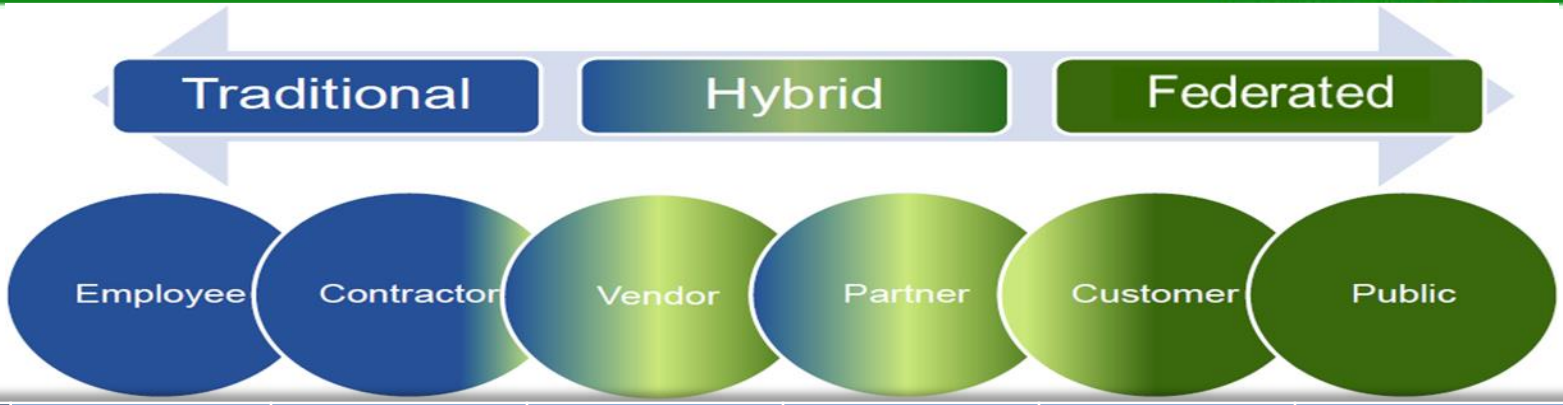
Contractual & Policy Control Points

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



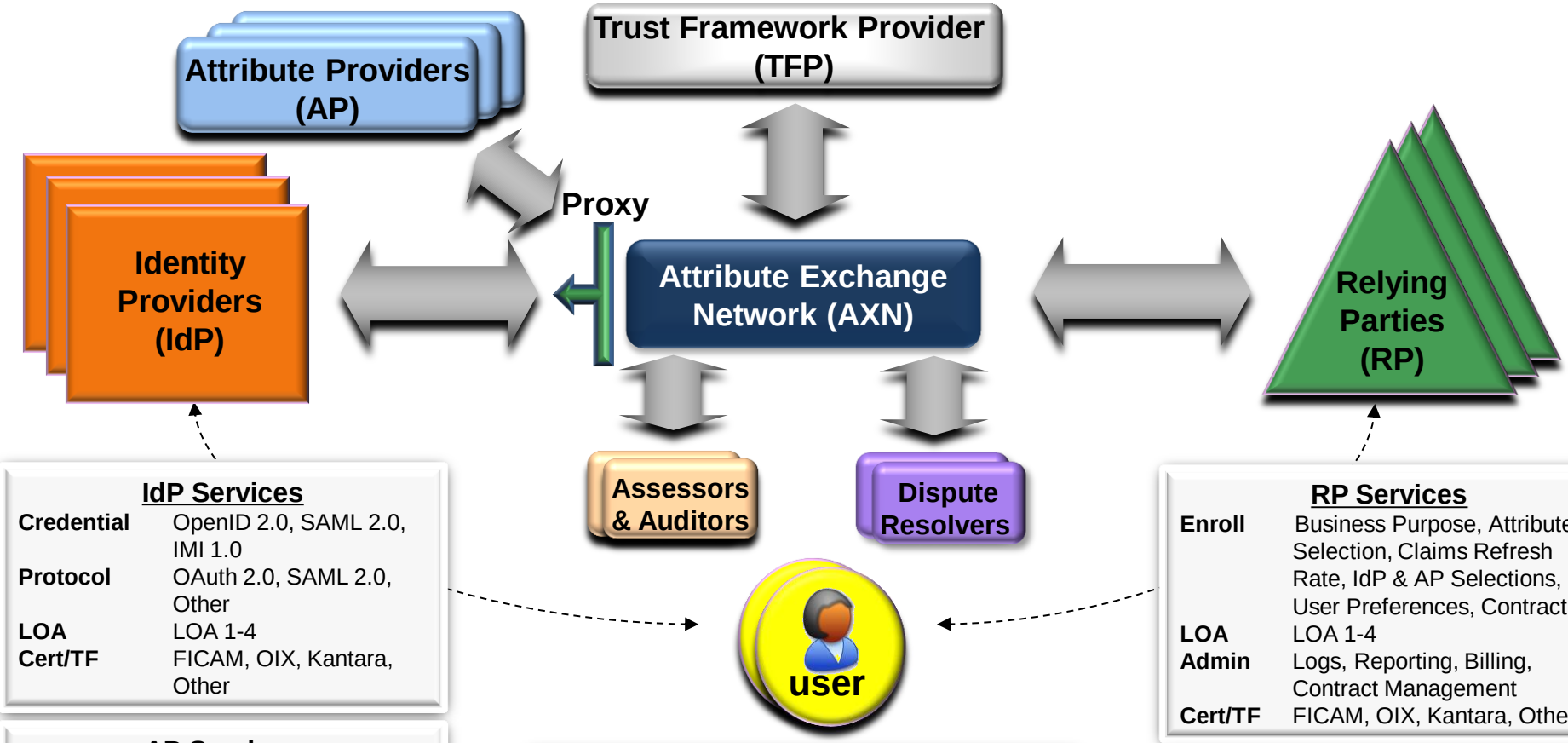
IdAM Constituency To Approach



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**	Username/Pswd/ Strong Auth/ **Federate/ Adaptive Access/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



IdP Services

Credential	OpenID 2.0, SAML 2.0, IMI 1.0
Protocol	OAuth 2.0, SAML 2.0, Other
LOA	LOA 1-4
Cert/TF	FICAM, OIX, Kantara, Other

RP Services

Enroll	Business Purpose, Attribute Selection, Claims Refresh Rate, IdP & AP Selections, User Preferences, Contract
LOA	LOA 1-4
Admin	Logs, Reporting, Billing, Contract Management
Cert/TF	FICAM, OIX, Kantara, Other

AP Services

Attributes	N, E, A, T, SS, DOB, Gender, Corp Verification
Quality	Refresh Rate, Coverage, Sources, Data Types
Physical	Device ID, BIO, Other
Pricing	Per Transaction, Per User Per Year, Annual License
Cert/TF	FICAM, OIX, Kantara, Other

AXN Services

Billing	Pricing and Analytics
Acct Management	Service Provisioning
Contracting	Policy Management
Marketing	Transaction Management
Registration	Operations and Security
Logs, Reporting	Administration
Audit	User Interface

User Services

Attributes	Not Stored In AXN, Self Asserted, Data Minimization
PDS	PII, Preferences, ABAC, Encrypted, External Store
MAX	User Only, Personal Control and Security, Acct Linking, Federated Access Via RP

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, Retinal, 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
PII	Name+ Email+ Address+ Telephone (NEAT)	TMI + DOB	TM2 + SSN4	TM3 + SSN9
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

Low — Cost — Higher

Low — Cost — Higher

Criterion-FCCX-03

AXN Business Services

- **Credential Transaction Management**
  - IDP authenticates user credentials as a service for RPs on the AXN
  - RP credential requirements for a given LOA (e.g., 1 – 4), type (e.g., SAML, OpenID, IDI), and trust framework
- **Attribute Verification and Claims Management**
  - RPs designate which attributes they required from users
  - User asserted, verified attributes and claims are shared with RPs with user permission
  - Device ID and biometric attributes are verified as required for RP authorization
- **Preference Management**
  - RPs designate preferences for users when interacting with the RP service
- **Attribute Based Access Control (ABAC)**
  - RP policy controls limit user access to resources based on verified, user-asserted attributes
- **User Managed Access (UMA)**
  - UMA services enable users (as resource owners) to control protected-resource access by requesting parties
  - Resource owners can manage and delegate resource sharing based on ABAC

Trust Economics

Efficient Online Identity Ecosystems Drive Markets Faster/Further

Reliability + Repeatability = Trust ➡ Predictable Behavior ➡ Metrics & Benefits

Use of Verified Attributes ➡ Increases Trust ➡ Decreases Friction

Quantitative Trust = ⬆ Revenue

Metrics	Benefits
⬆ Speed	Expand Existing Markets
⬇ Costs	Enable New Services
⬇ Risk	Mitigate Fraud
⬆ Transactions	Competitive Differentiation

Qualitative Trust ~ ⬆ Brand Value

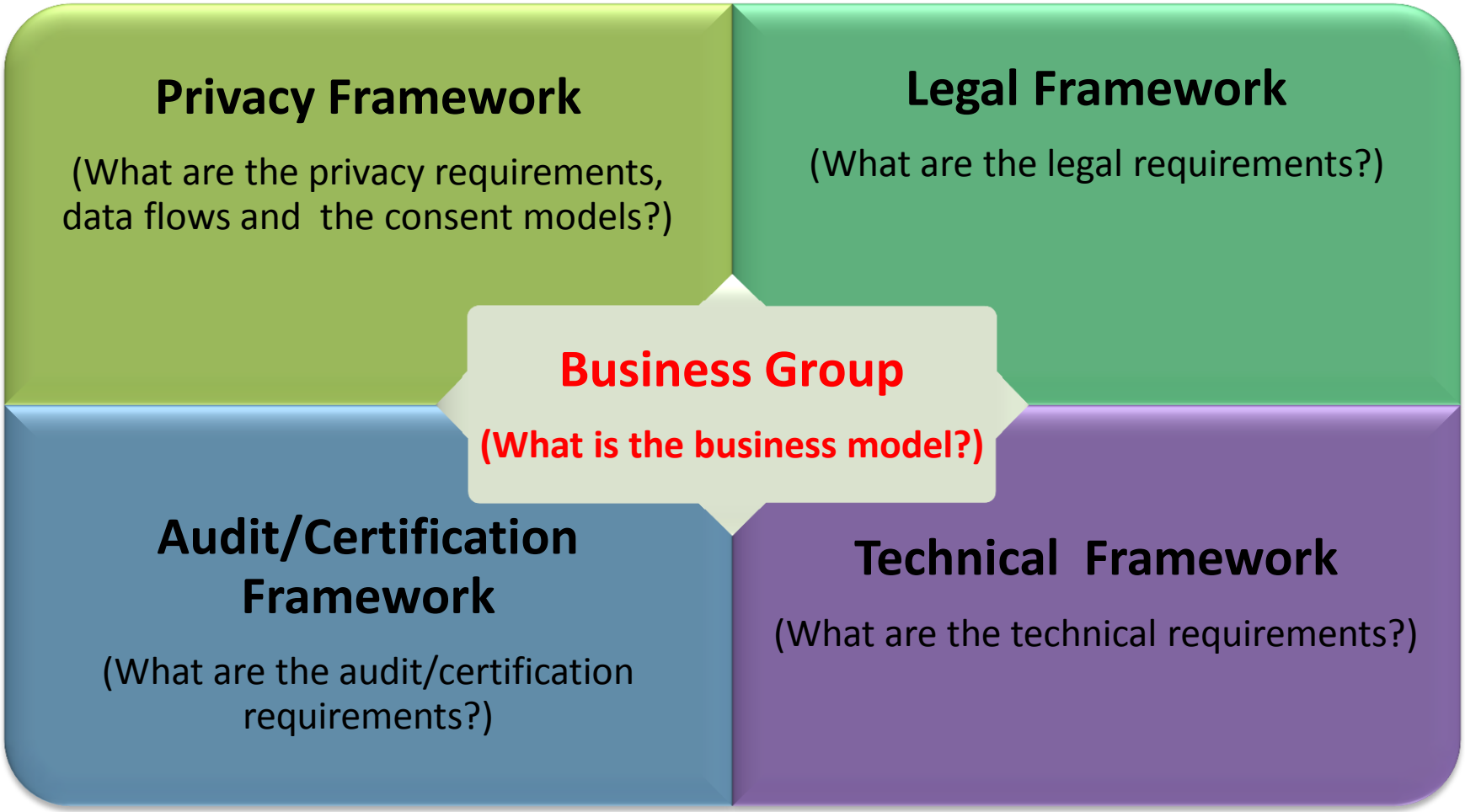
⬆ Perceptions of transparency, security and privacy

AX Trust Frameworks – A Definition

An Attribute Exchange (AX) Trust Framework ***enables*** a party who accepts a digital identity credential (called the relying party) to ***trust*** the identity, security, and privacy policies of the party who issues the credential (called the identity provider) and vice versa.

An AX Trust Framework is the tools, rules and business policies that enable *assurance* …

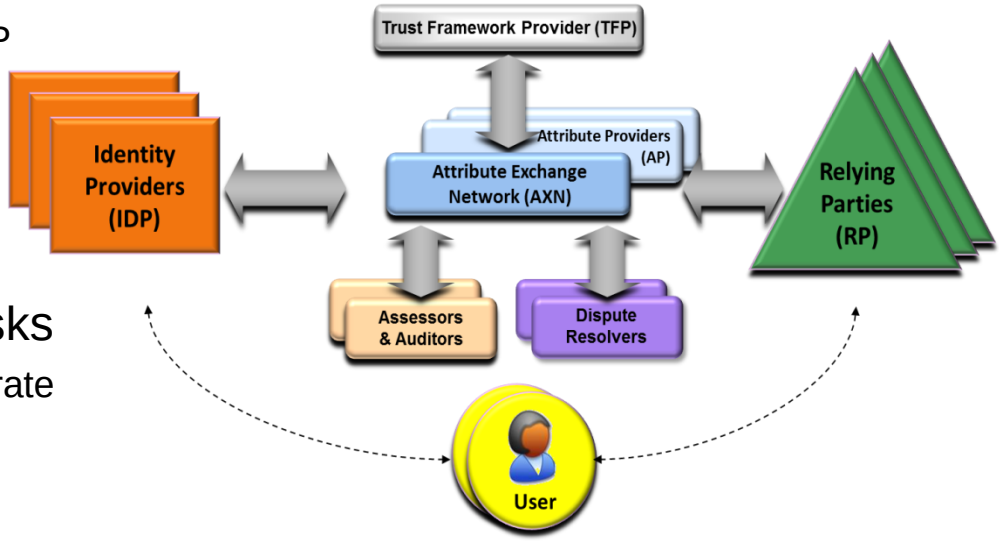
Anatomy of Trust Framework Development



TFP Project Implementation

Multiple Tasks Must Be Deployed As Parallel Activities

1. Trust Framework Provider (TFP) Implementation Tasks – Full Cycle
   - TFP and IDW leadership
   - Engage leadership and resources from TFP participants
2. TFP Business Model Strategy
   - Funding, ownership and cash flows
   - Partner contributions
3. Short Term TFP Implementation Tasks
   - Business plan, capital formation and corporate documentation
   - Legal Agreements
   - Messaging, marketing and meetings
4. Implement AXN Requirements
   - TFP supply chain use cases
   - TFP membership use cases
   - ABAC use cases



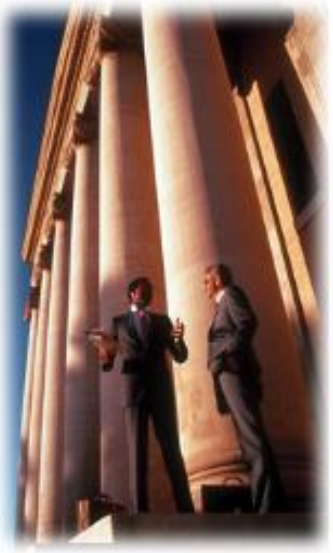
Seed Funding Is Required Until TFP Is Funded and Operational

TFP Implementation Tasks – Full Cycle

1. Identify industry sectors ideally suited for an Attribute Exchange (AX) Trust Framework (TF)
2. Develop TF ***risk mitigation policies***, use-cases, services and requirements (business, legal, technical, privacy/policy, assessor/certification)
3. Identify appropriate data (attribute nomenclature) standards and data sources (self-asserted, derived, direct from source)
4. Identify industry specific compliance requirements and regulations
5. Model TF participant benefits and monetization strategy
6. Develop TF participant enrollment strategy (including messaging, marketing, sales and PR)
7. Implement customized AXN requirements
8. Implement Trust Framework legal agreements
9. Engage in AX pilots at this stage as appropriate
10. Implement production operations

TFP Potential Business Strategy:
Funding, Ownership & Cash Flows

- Establish a Trust Framework Provider (TFP) corporate entity
  - TFP founders to have controlling interest after capital raise
- Fund TFP to implement tasks and to scale resources/staff
  - For example: the operations arm of 5 to 10 industry participants invest for a share of LLC equity to capitalize requirements
  - Participants also bring soft $ to minimize funding requirements
    - LLC could provide some funding back to participants to pay for soft costs (business/marketing & technical)
- Revenue Modeling (Example)
  - AXN distributes a % of net TF transaction revenues to TFP to return investment capital plus a yield
  - Subsequent AXN distributions TBD - TFP splits net with partners (or builds equity)
- Target TFP valuation multiple – 5 to 10 x revenues

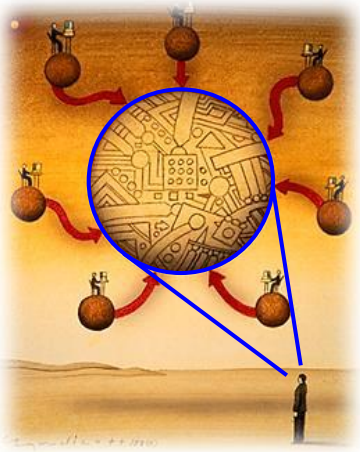


TFP Potential Business Strategy:
Partner Contributions

- TFP
  - TFP market opportunities, leadership and contacts
  - Resources – business, legal, technical, privacy
  - Seed funding for TFP to implement first tasks and to raise capital (<$5M)
  - Capital structure and participant funding
  - TFP operations management and leadership

- ID Dataweb (IDW)
  - Attribute Exchange Network (AXN) services and participants
  - AXN business model, contracts and adjacent market opportunities
  - Identity industry ecosystem contacts & expertise
  - NSTIC pilot project – potential for some government funding for pilots and international PR

Implement AXN Requirements



- TFP Membership Requirements
  - TFP Governance and Policy Structure (COR)
  - Business, Legal, Technical, Privacy/Policy Interoperability
  - Credential Trust Elevation & Monetization Services
  - Certification and Accreditation Requirements

- Enterprise Use Cases
  - Contextual Trust Elevation with Attribute Verification Services
  - Preference Management Interface in User Admin Console (MAX)
  - Enterprise ABAC and UMA Services

Next Steps

- Implement first TFP entity
- Secure seed funding for TFP project(s)
- Develop TFP materials for capital raise
  - Refine business plan
  - Marketing presentation
  - Financial proforma
  - Legal documentation
- Implement AXN requirements
- Engage in pilots as appropriate
- Implement production operations