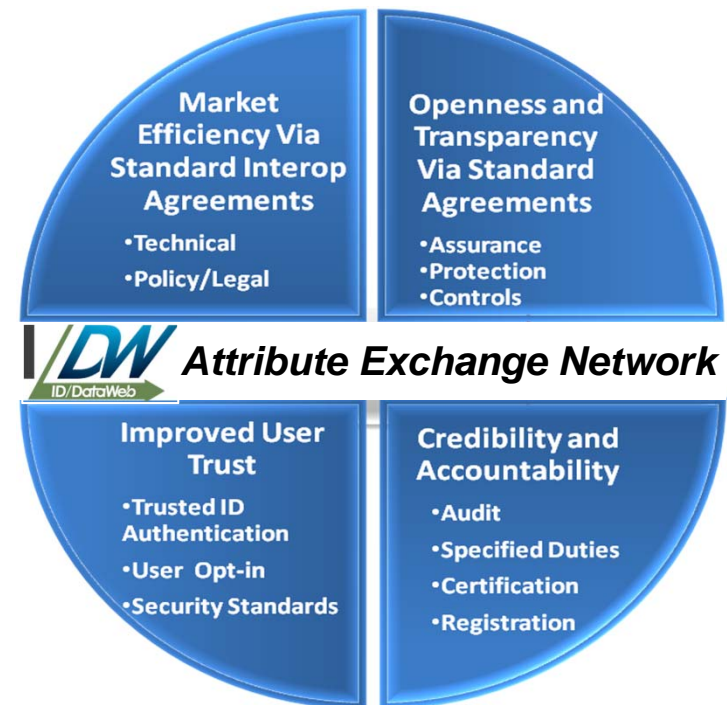




## ***Online Identity Attribute Exchange 2014 Initiatives***

# Agenda

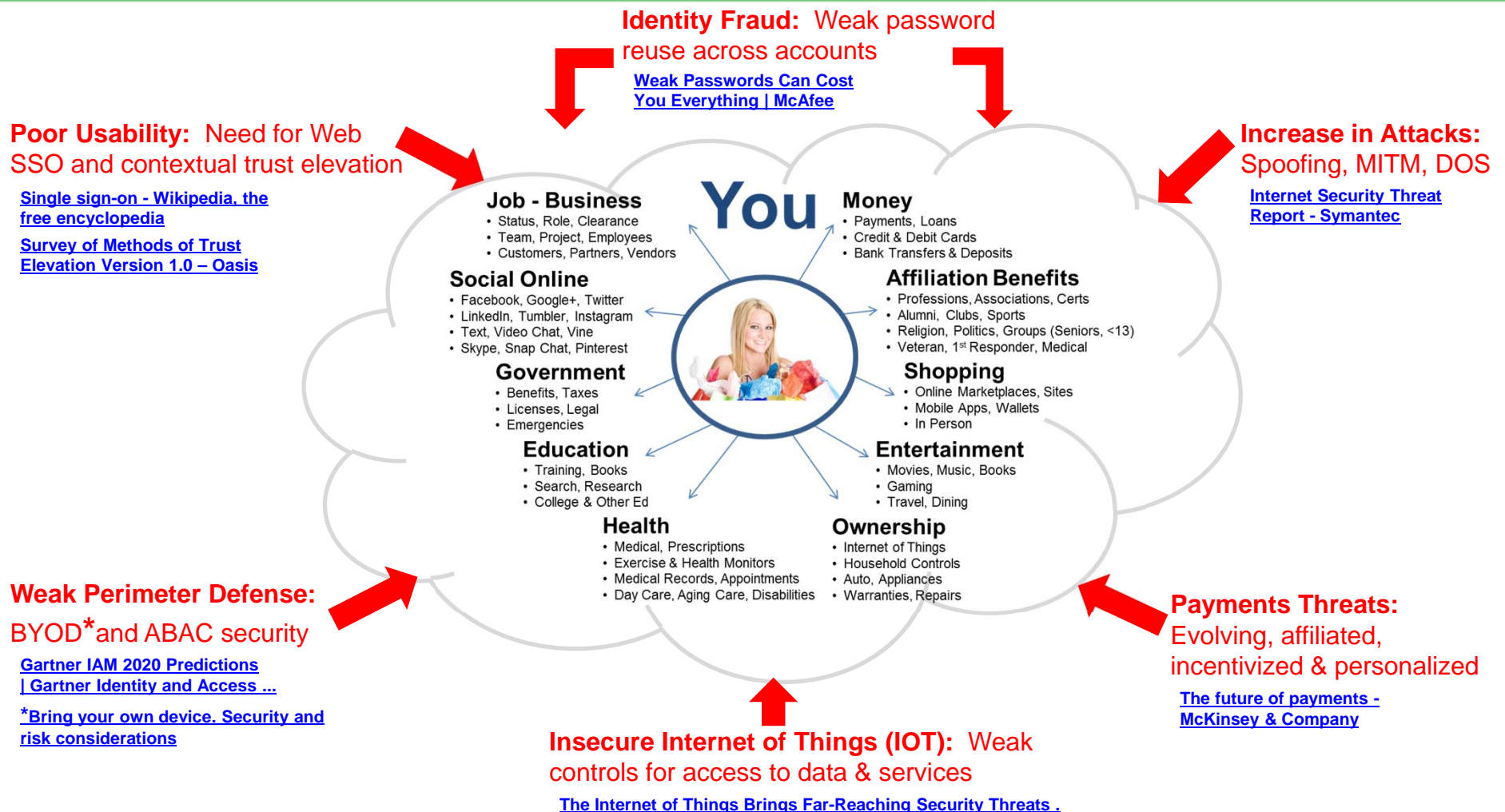
- Overview
- AXN Services Framework
- Demonstration
- Use Cases
- Business Model
- Summary



## Key Concepts

- ✓ A user's identity is comprised of their personal (PII), biometric, device and affiliation attributes.
- ✓ The more attributes that can be verified - the greater the assurance (security) associated with an identity.
- ✓ With the User's permission, after their attributes are verified, these attributes are made available to securely access online services (from AXN customers such as Census, Broadridge, GE, AARP).
- ✓ Users control and securely manage their attributes via the AXN.
- ✓ Online services are charged a fee each time a user's attributes are verified. This service is free to users.

# Online Identity Today Is Broken



**What's Needed?** *Trusted, Interoperable, User-Centric Identity*



# Attribute Exchange Network (AXN)

## 1. Bring Your Own Identity (BYOID)

- Fewer identities for cross-site usage with Trusted, interoperable SSO
- User affiliation benefits drive adoption
- Contextual trust elevation with multi-factor device ID, biometrics as needed
- Attack mitigation - spoofing and MITM
- Attribute Based Access Control (ABAC)

## 2. Credential Federation

- Verified attributes for binding to new or existing user accounts
- Reduces drop off, account creation and maintenance costs

## 3. Neutral Marketplace

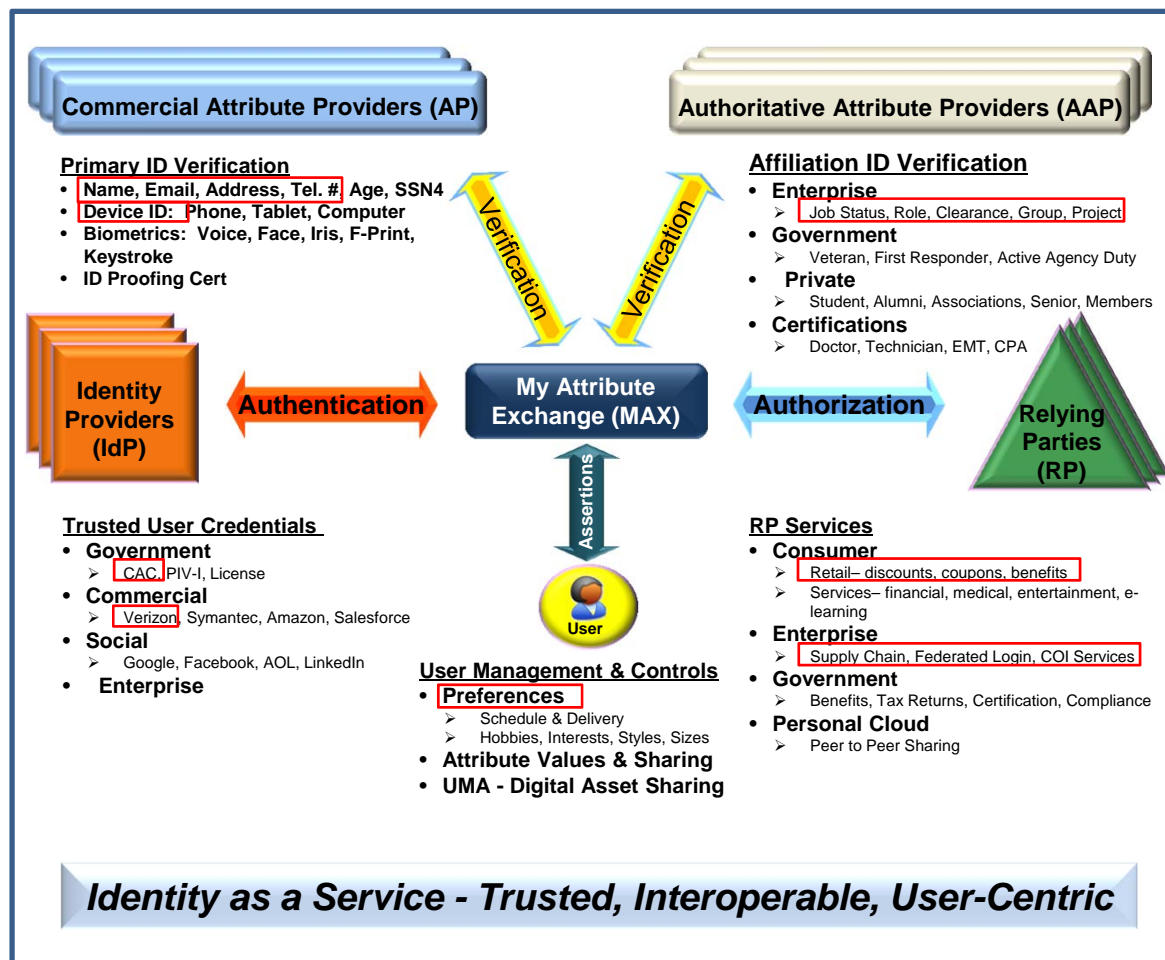
- Open, competitive exchange – best of breed and value
- Free to users; lowers RP costs; a new channel for IdPs and APs

## 4. Contractual and Policy Hub

- One AXN contract to access competitive AP and IdP services

## 5. Privacy by Design

- User opt-in, User Management Console, and data minimization
- AXN is a transaction proxy with no central data store of user PII



### OIX AX Trust Framework

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

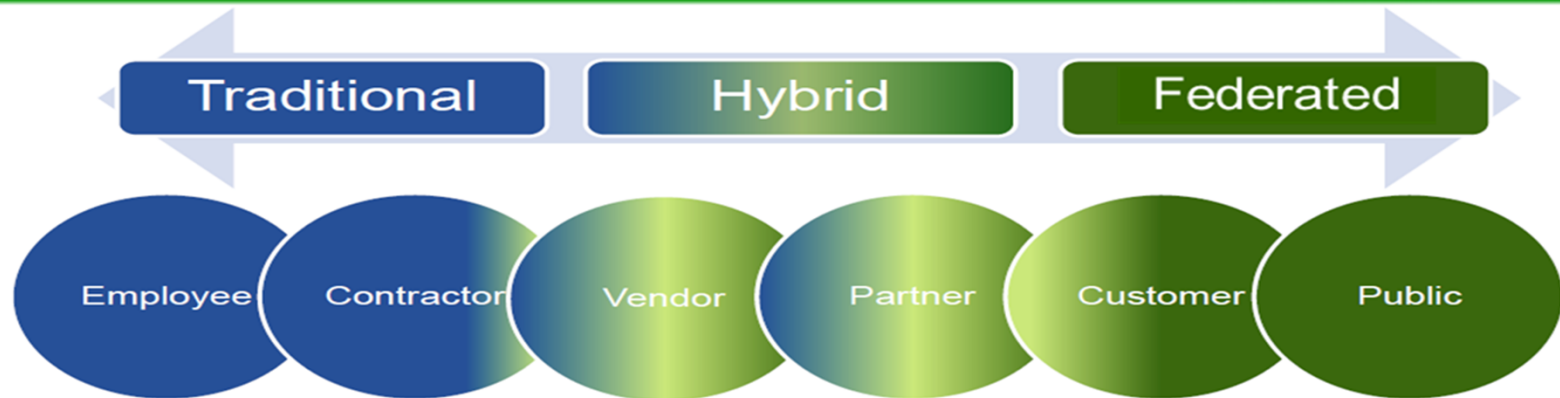
# Current AXN Providers and Roles



Role	Current Provider on the Exchange	Description of Service
<b>Identity Providers</b>	<b>LOA 3+:</b> Lockheed Martin, Raytheon, Boeing, Verizon, Symantec* <b>LOA 1:</b> Google, AOL, Facebook, Amazon, LinkedIn, PayPal, Salesforce, Microsoft, Box, Evernote	Credential Authentication Services
<b>Attribute Providers (PII Verification)</b>	Experian, LexisNexis, Pacific East, Enterprise LDAP/Directories*, Equifax, Telesign, ORC*, Acxiom*	Traditional validation of user PII (Name Address, Telephone, DOB, and Social)
<b>Device ID</b>	Telesign, Wave, 41 <sup>st</sup> Parameter*, Authentify*, SecureAuth*	Identification of the access device via the PIN, TPM chip, software download, or other means
<b>Biometrics</b>	Daon, MorphoTrust*	Services are capable of voice, face and other like recognitions at varying degrees of sophistication
<b>Signature/ Key Stroke Dynamics</b>	Kaje, Authenware	Alternative signature capture
<b>Document Proofing</b>	ID Checker*, Experian*	Confirms that a government issued document is legitimate and matches the user PII

\* Currently in integration and testing

# 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 <b>or</b> <b>Federated</b> Source	Delegated Admin/ <b>Self-</b> <b>service/Federated</b> <b>Provisioning -SCIM</b>	Delegated Admin/ <b>Self-</b> <b>service/Federated</b> <b>Provisioning -SCIM</b>	Self Service/ <b>Social</b> <b>Identity (OpenID)/</b> <b>Federated</b> <b>Provisioning -SCIM</b>	Self Service/ <b>Social</b> <b>Identity (OpenID)/</b> <b>Federated</b> <b>Provisioning -SCIM</b>
ID Store	Enterprise Directory	<b>Federated</b> Enterprise Directory	<b>Federated</b> Enterprise Directory/ <b>VDS</b>	<b>Federated</b> Enterprise Directory/ <b>VDS</b>	<b>Federated</b> Enterprise Directory/ <b>VDS</b>	<b>Federated</b> Enterprise Directory/ <b>VDS</b>
Authorization	Roles/Rules/ <b>ABAC</b>	Sponsored Roles/Rules/ <b>ABAC</b>	Roles/Rules/ <b>ABAC</b> <b>/OAuth or SAML</b>	Roles/Rules/ <b>ABAC</b> <b>/OAuth or SAML</b>	Roles/Rules/ <b>ABAC</b> <b>/OAuth or SAML</b>	Roles/Rules/ <b>ABAC</b> <b>/OAuth or SAML</b>
Authentication	Username/Pswd/ Strong Auth/ <b>Federate/ID</b> <b>Proofing</b>	Username/Pswd/ Strong Auth/ <b>Federate/ Adaptive</b> <b>Access/ID Proofing</b>	Username/Pswd/ Strong Auth/ <b>Federate/ Adaptive</b> <b>Access/ID Proofing</b>	Username/Pswd/ Strong Auth/ <b>Federate/ Adaptive</b> <b>Access/ID Proofing</b>	Username/Pswd/ Strong Auth/ <b>Federate/ Adaptive</b> <b>Access/ID Proofing</b>	Username/Pswd/ Strong Auth/ <b>Federate/ Adaptive</b> <b>Access/ID Proofing</b>
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 Demonstration



# Customer / B2C Use Case

## Registration Process

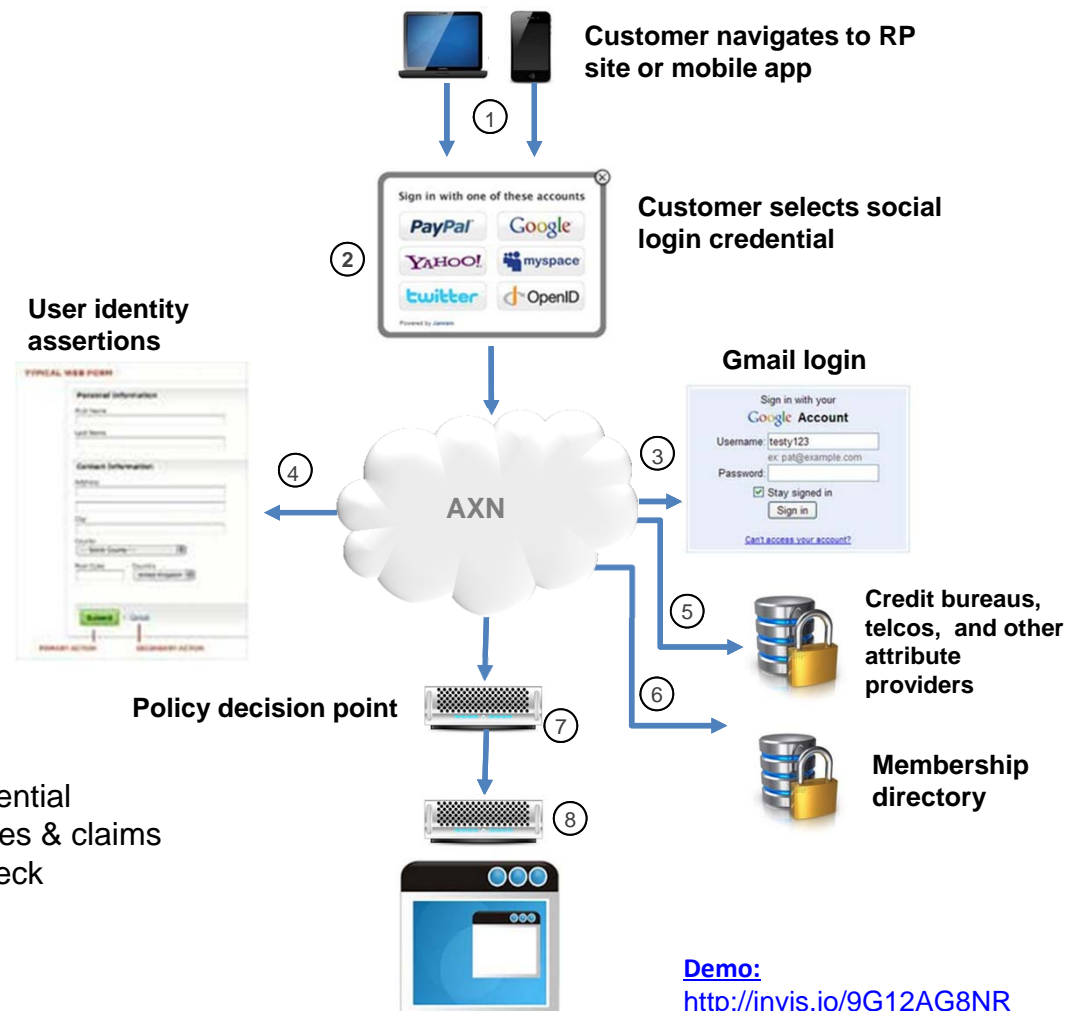
1. User downloads (or navigates) and starts RP app
2. User selects ID for registration
3. User logs in at IdP via AXN proxy service
4. AXN collects user data, including RP membership assertion
5. AXN verifies user data and, as needed, records device identity (trusted device)
6. AXN verifies RP member status against Enterprise membership directory
7. AXN passes result to policy decision point
8. Policy decision point grants access to app

## Subsequent Logins

- Refresh user's attributes (AXN as needed)
- Verify device identity (as needed)

## Benefits

- Privacy and security enhancing process
- Mitigates spoofing and man-in-the-middle attacks
- Eliminates need for customers to create a new credential
- Federate login to other services with verified attributes & claims
- Enables optional device identity and/or biometric check





# Broadridge - WHO WE ARE



## A Financial Industry Communications Hub

3 billion distributions annually  
across North America, proprietary technology  
drives 60% + suppression rates

950+  
Banks & Brokers



550+  
Mutual funds



Institutional  
investors



Retirement Plans,  
VA's/TPA's



12,000  
Corporate issuers



140,000,000 +  
Individual Accounts

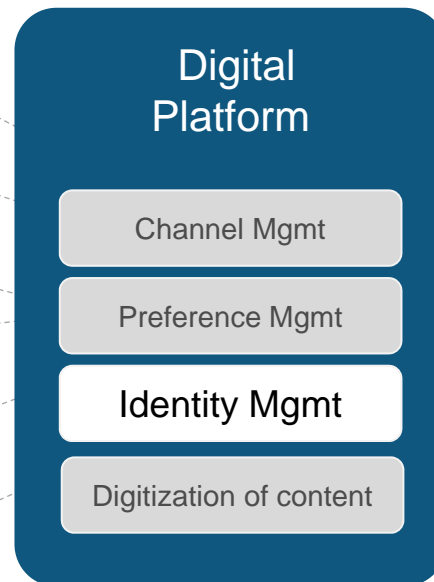
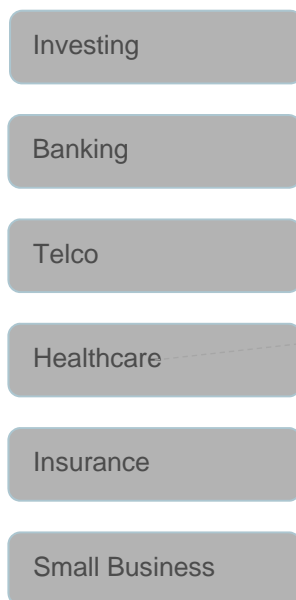


# Broadridge - THE POWER OF IDENTITY

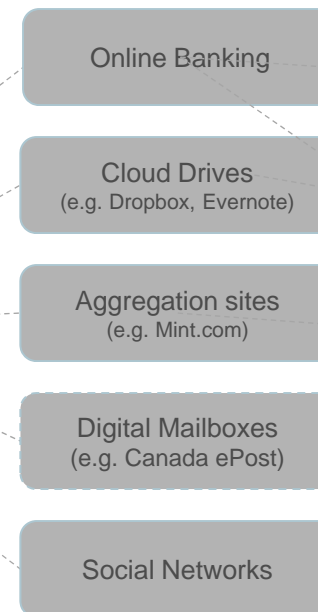


Identity is the glue in our model to enable consumer adoption

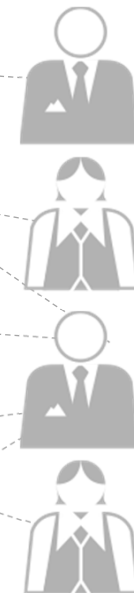
Brands (i.e. mailers)



Channels



Consumers



- Brands across multiple verticals participate
- Brands have one integration point
- Brands control security (a federated model, as brands store data behind their firewalls)

- Platform connects to the channels brands support and consumers are using

- Consumers control how they receive content from channels they are already using

# B2C2B Service Federation Use Case

## Registration Process

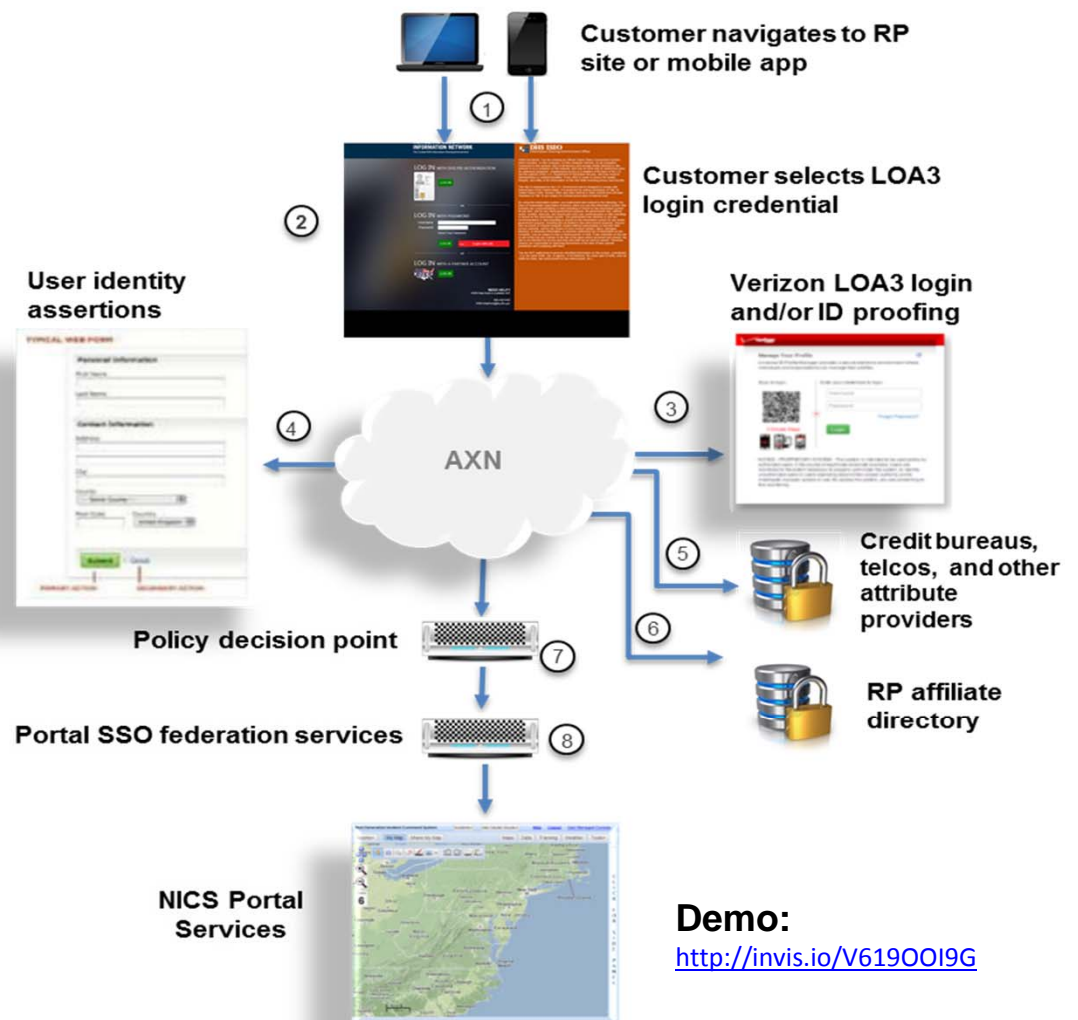
1. User downloads (or navigates to) and starts RP app
2. User selects ID for LOA3 registration
3. User logs in at IdP (leverage ID proofing & credential issuance Use Case as needed)
4. AXN collects user data, including RP affiliation assertion
5. AXN verifies user data and, as needed, records device identity (trusted device)
6. AXN verifies RP member status against Enterprise membership directory
7. AXN passes result to policy decision point for RP app
8. User evokes federated portal service and redirects for SSO at LOA3

## Subsequent Logins

- Refresh user's contextual attributes (as needed)
- Verify device identity (as needed)

## Benefits

- Privacy and security enhancing process
- Eliminates need for customers to create new LOA3 enterprise credentials
- Enables optional device identity check
- SSO to federated LOA3 services



# Partner / B2B & ABAC Use Case

## Registration Process

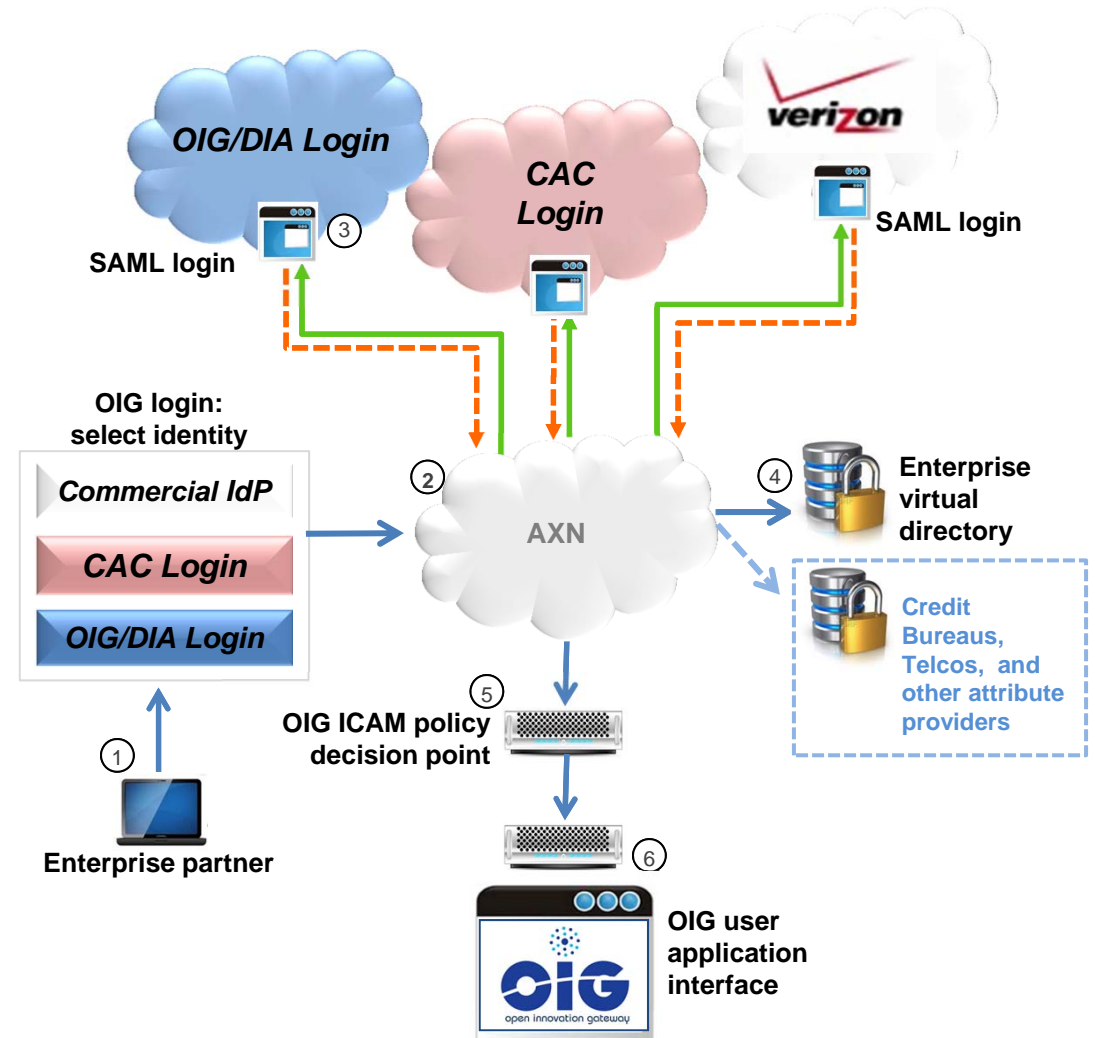
1. User navigates to login to OIG application; redirects to IdP login page
2. User redirect to AXN
3. User redirect via SAML to IdP of choice to login (e.g., UN/PW credential)
4. Identity proofing via AXN
  - Verify user's contextual info - name, email, office location, clearance, etc.
  - Verify Enterprise / Partner project info
5. Pass results to OIG ICAM policy decision policy point
6. On successful authentication, pass user to OIG app

## Subsequent Logins

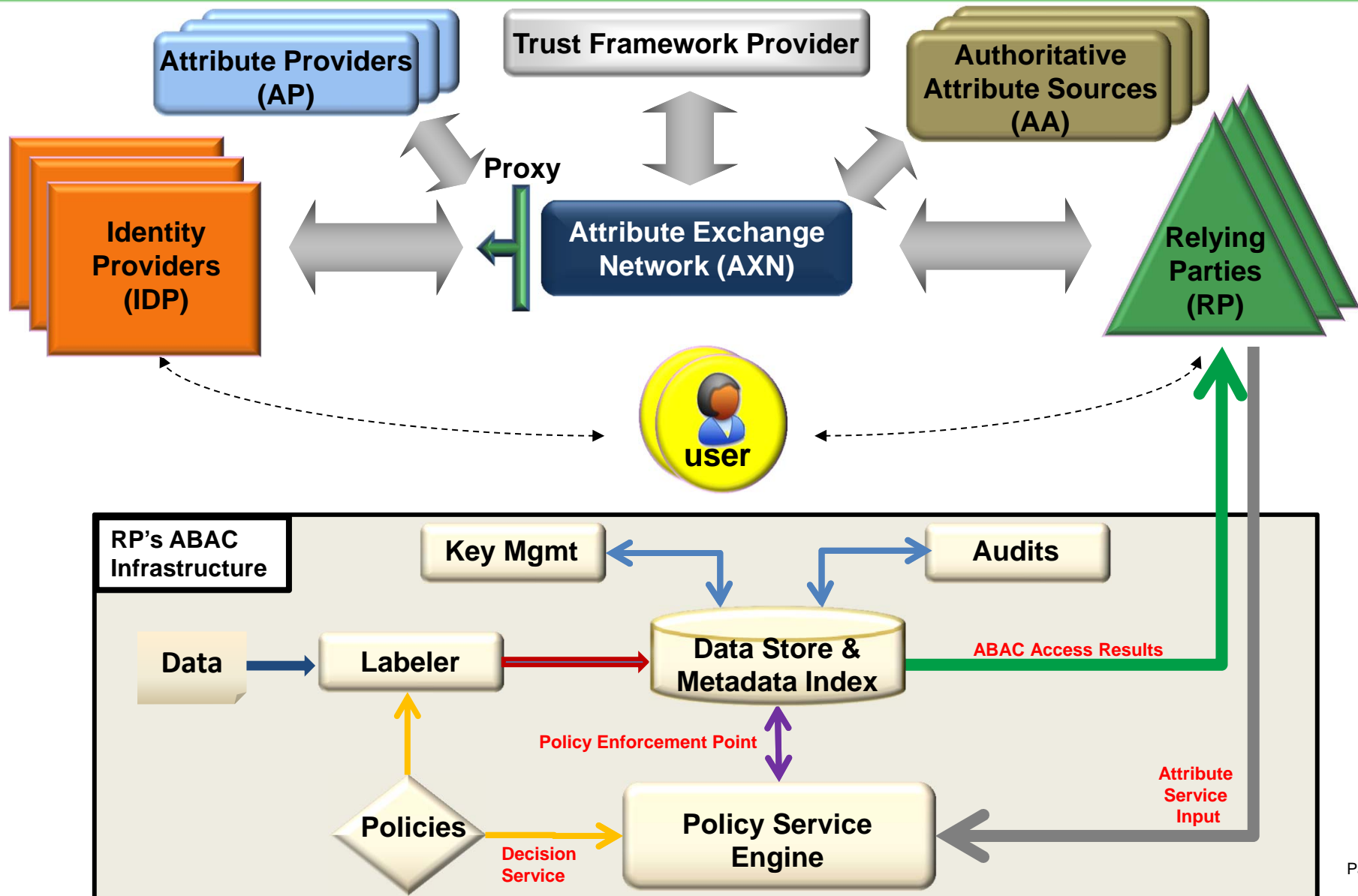
- Verify user's contextual info
- Verify device identity
- Check device geo-location
- AXN refreshes user's attributes (as needed)

## Benefits

- Eliminates need to issue SSOs to partners
- Incorporates contextual info for ABAC
- Incorporates device identity & location for added security



# AXN - ABAC Ecosystem





# B2C Sponsor/Affiliation Use Case

## Registration Process

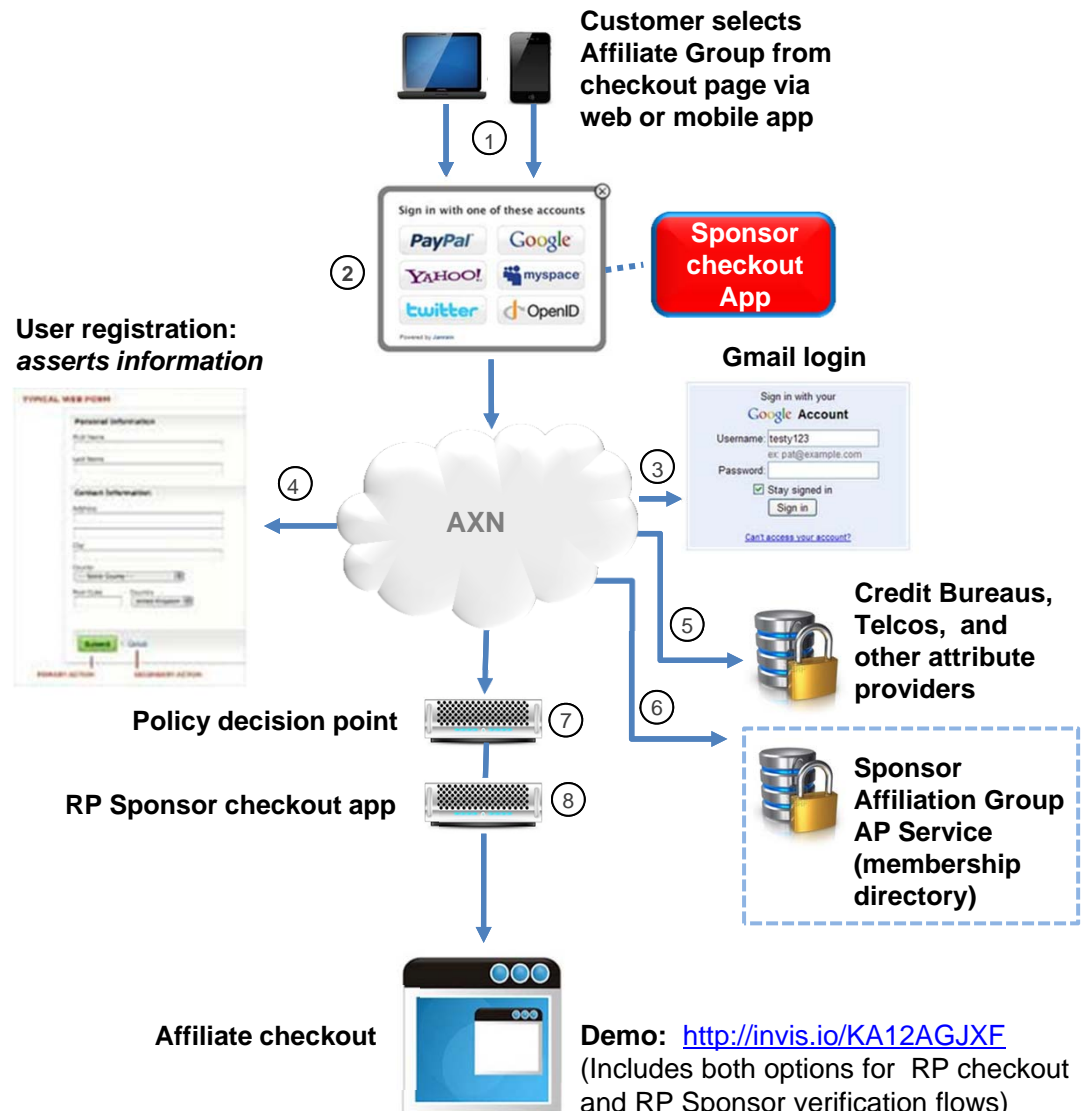
1. User navigates to Affiliate checkout page after selecting items to purchase
2. User selects Identity for registration login to RP checkout app
3. User logs in at IdP (or cookie evokes login)
4. AXN collects user data and any additional Sponsor Affiliation Group information
5. AXN verifies user data, and as needed, location and records trusted device identity
6. AXN verifies affiliation status with RP Affiliation Group AP service
7. AXN passes result to RP Sponsor checkout app policy decision point
8. RP Sponsor checkout app calcs discount, collects payment and redirects to Affiliate

## Subsequent Logins

- Refresh user's attributes (AXN as needed)
- Verify device identity & location (as needed)

## Benefits

- Easy to deploy
- Checkout controlled securely by RP Sponsor
- Verified user attributes through privacy enhancing process
- Offers easy access and helps drive membership / benefits
- Members can renew membership when trying to secure a discount



# IdP Proofing Use Case: *RP Redirect Via AXN to IdP*



## Registration Process

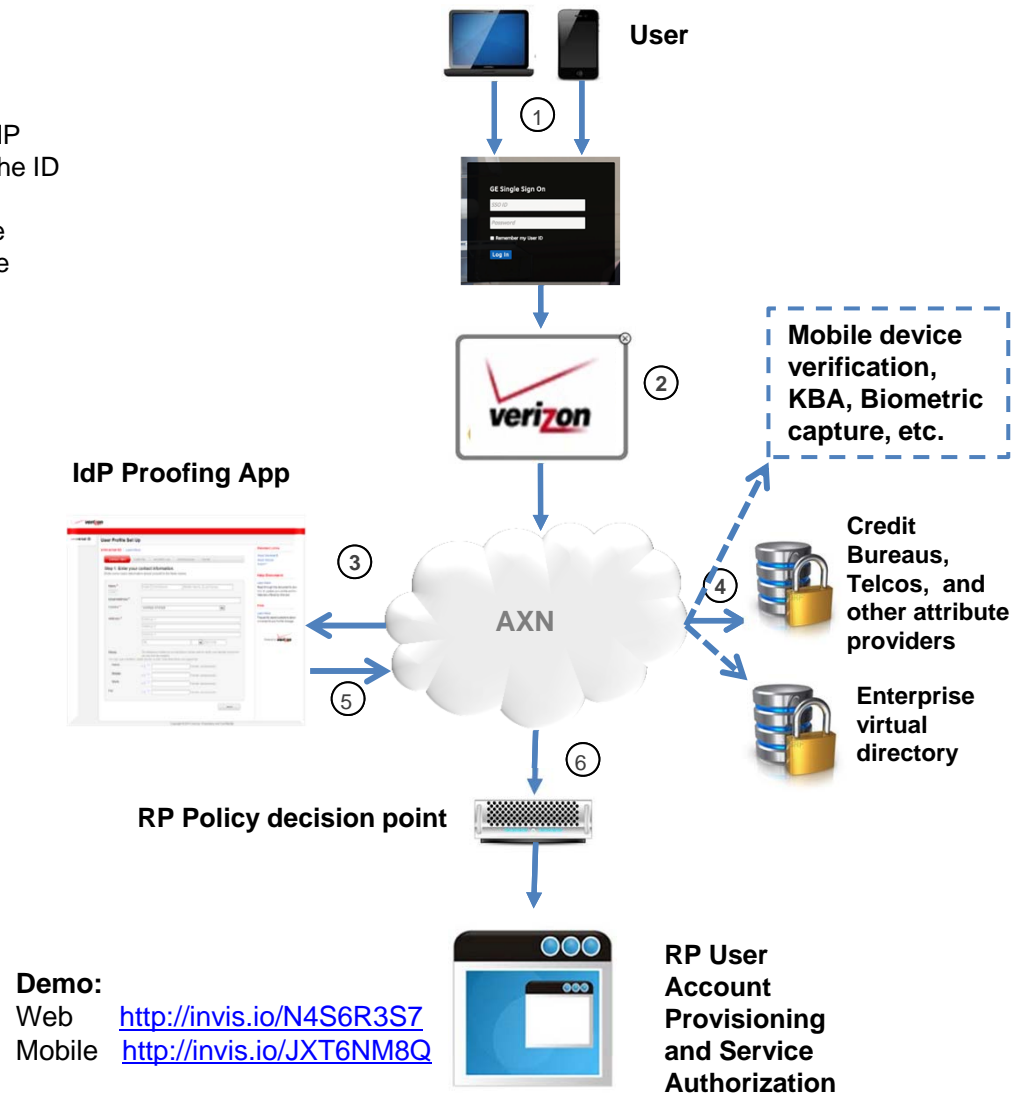
1. User accesses RP site to access service and create an account
2. User selects IdP to create a credential and undergo ID proofing
3. AXN redirects user to Logon App and new users redirect to the IdP Proofing App to create an account and assert user attributes for the ID proofing process
4. AXN verifies user asserted attributes and can trigger KBA, mobile device verification, biometric capture or/and contextual enterprise attribute verification
5. On success, AXN associates credential with attribute assertions, device identity, biometric attributes, and any attribute claims
6. AXN passes results to RP policy decision point for user account creation and service authorization

## Subsequent Transactions

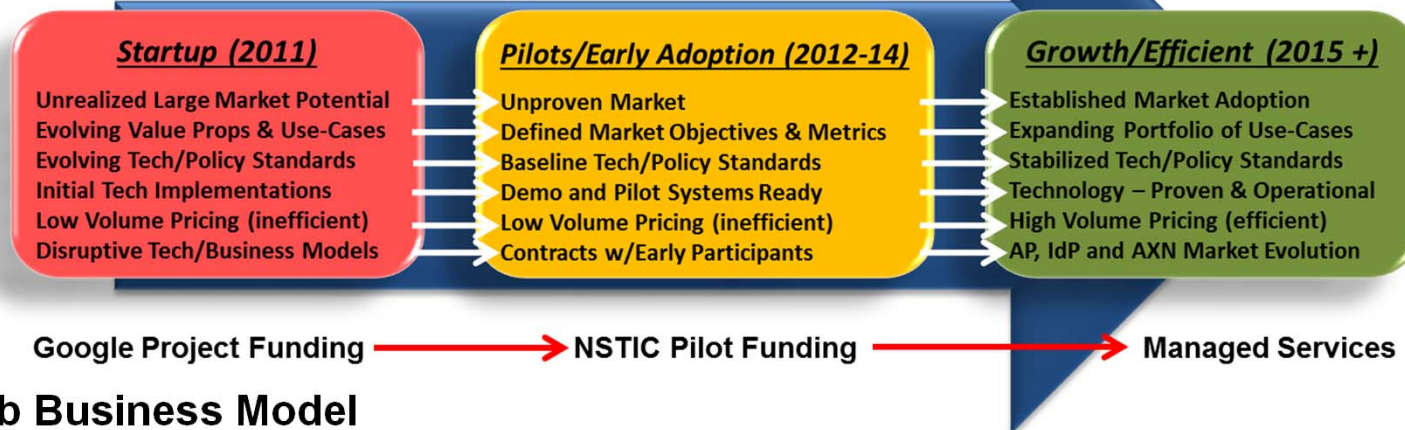
- IdP authenticates user logins
- AXN verifies device identity (and/or contextual attributes)
- User attributes get refreshed per IdP policy

## Benefits

- One AXN contract to procure competitive attribute verification, KBA, biometric and device ID services
- IdP can re-use (without charge) the credentials, attributes and claims
- Credentials exist on the AXN for federated authentication services and monetization
- Introduces contextual authentication with credential and enterprise attributes



# ID Dataweb Summary

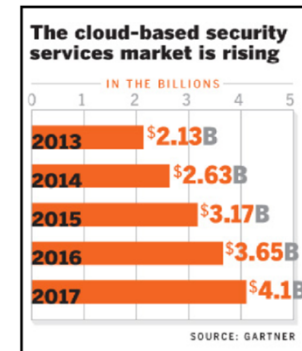


## ID Dataweb Business Model

- Operate the Attribute Exchange Network (AXN) – **trusted, interoperable, user-centric identity as a service**
  - Optimized for community/customer/partner identity federation
  - Marketplace for credential and attribute verification services

## AXN Revenue

- Baseline Managed Services** (priced per transaction or per user/year)
  - Credential Federation and Attribute Verification – all markets
    - Reseller of Attribute Provider (AP) and Identity Provider (IdP) services
    - Setup and minimum transaction fees
- Value-Add Managed Services** (priced per transaction or per user/year)
  - Affiliate (benefits/discounts) - communities and retailers
  - Payments and Insurance - online and mobile e-commerce
  - Identity Proofing - IdPs and enterprises
  - Preference Management - all markets
  - Attribute Based Access Control (ABAC) – all markets
- Transaction Data Analytics & Risk Management Services (long term)**



## Growing Addressable Market

- Cloud-based Security Services:** \$2.1B in 2013 to \$3.1B in 2015 (*Gartner*)
- IDaaS:** Growing from \$500M to \$1.24B in 2017 (28.3% annual growth) (*Gartner*)
- Global Cloud Security:** \$4.20B in 2014 to \$8.71B in 2019

# Summary



- 2014 - 2015 AXN initiatives:
  - 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 – embraces and leverages legacy business models, regulations and technologies



# AXN Benefits Summary



- **Relying Parties (RPs)**
  - **Credential Federation:** reduces drop off, account creation and maintenance costs with service appropriate credentials
  - **ICAM Strategy:** optimize risk mitigation, privacy, and user experience for each constituency and service
  - **Authoritative Attribute Services:** affinity group marketing, ABAC and UMA
  - **Preference Management Services:** user managed CRM
  - **Contractual Hub:** contract efficiencies to implement price competitive, efficient, exchange services
  - **Transaction Security:** contextual trust elevation, BYOD management, ABAC and UMA
  - **User Privacy:** user opt-in, proxy services, data minimization, no central data store, UMC
  - **Trust Framework Infrastructure:** standards-based policy interoperability and management
- **Identity Providers (IdPs)**
  - **Identity Proofing:** competitively source attribute verification, KBA, biometric, and device ID services via the AXN via a single contract
  - **Credential Provisioning:** AXN-proofed credentials are automatically available for RP account creation, and IdPs can monetize credentials as users create multiple new RP account easily
  - **Market Coverage:** online AP registration, contract administration and service provisioning
- **Attribute Providers (APs)**
  - **Market Model:** enables both competitive market exchange and proprietary AP client models
  - **Online Channel:** reseller exchange expands market reach and revenues for AP services
- **Users**
  - **User Experience:** reduces username/passwords, free, privacy enhancing, secure, and easy to use



# 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
Low ↓ Cost Higher	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		

Criterion-FCCX-03