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
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

<table>
<thead>
<tr>
<th>Industry</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadridge Use Case</td>
<td>B to C</td>
</tr>
<tr>
<td>RP Service: Fluent – Online Application Platform for Investor Communications</td>
<td>Investor Communications</td>
</tr>
<tr>
<td><strong>Industrial Enterprise Use Case</strong> (Pending Final Approval)</td>
<td>B to C, B to B</td>
</tr>
<tr>
<td>RP Service: Various Service Sector Applications Corporate, Partner and Consumer Account Access</td>
<td>Multiple Market Verticals</td>
</tr>
<tr>
<td><strong>DHS/FEMA (MIT Lincoln Labs) First Responder Use Case</strong></td>
<td>G to G, G to C</td>
</tr>
<tr>
<td>RP Service: Account creation and login for the First USA disaster response collaboration portal</td>
<td>First Responders First USA Services</td>
</tr>
<tr>
<td>eBay Use Case</td>
<td>B to C, C to C</td>
</tr>
<tr>
<td>RP Service: Retail Seller and Buyer Account Creation and Login</td>
<td>Retail</td>
</tr>
</tbody>
</table>
# IdAM Constituency To Approach

## Purpose/Posture
- **Employee Services**: Enable/Provide/Manage/Collect
- **Contractor Services**: Enable/Provide/Manage/Collect
- **Vendor Services**: Enable/Manage/Collect
- **Partner Services**: Enable/Provide/Support
- **Customer Services**: Expose/Sell/Service/Provide
- **Public Services**: Expose/Sell/Service/Provide

## Life Cycle Event / Options
- **Employee Services**: Delegated Admin/Change in Authoritative Source
- **Contractor Services**: Delegated Admin/Change in Authoritative Source
- **Vendor Services**: Delegated Admin/Change in Authoritative Source or Federated Source
- **Partner Services**: Delegated Admin/Change in Authoritative Source or Federated Source
- **Customer Services**: Delegated Admin/Change in Authoritative Source or Federated Source
- **Public Services**: Delegated Admin/Change in Authoritative Source or Federated Source

## ID Store
- **Employee Services**: Federated Enterprise Directory
- **Contractor Services**: Federated Enterprise Directory
- **Vendor Services**: Federated Enterprise Directory/VDS
- **Partner Services**: Federated Enterprise Directory/VDS
- **Customer Services**: Federated Enterprise Directory/VDS
- **Public Services**: Federated Enterprise Directory/VDS

## Authorization
- **Employee Services**: Roles/Rules/ABAC
- **Contractor Services**: Roles/Rules/ABAC
- **Vendor Services**: Roles/Rules/ABAC
- **Partner Services**: Roles/Rules/ABAC
- **Customer Services**: Roles/Rules/ABAC
- **Public Services**: Roles/Rules/ABAC

## Authentication
- **Employee Services**: Username/Pswd/Strong Auth/Federate/ID Proofing
- **Contractor Services**: Username/Pswd/Strong Auth/Federate/ID Proofing
- **Vendor Services**: Username/Pswd/Strong Auth/Federate/ID Proofing
- **Partner Services**: Username/Pswd/Strong Auth/Federate/ID Proofing
- **Customer Services**: Username/Pswd/Strong Auth/Federate/ID Proofing
- **Public Services**: Username/Pswd/Strong Auth/Federate/ID Proofing

## Audit
- **Employee Services**: Access Cert./Reporting
- **Contractor Services**: Access Cert./Reporting
- **Vendor Services**: Access Cert./Reporting/Real-time Monitoring
- **Partner Services**: Real-time Monitoring/Fraud Detection
- **Customer Services**: Real-time Monitoring/Fraud Detection
- **Public Services**: Real-time Monitoring/Fraud Detection

*Source: Gartner Group*
AXN Services Framework

Identity Providers (IdP)

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

Attribute Providers (AP)

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

Attribute Exchange Network (AXN)

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

Trust Framework Provider (TFP)

Proxy

Relying Parties (RP)

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

Assessors & Auditors

Dispute Resolvers

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, 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
AXN - ABAC Ecosystem

- Attribute Providers (AP)
- Trust Framework Provider
- Authoritative Attribute Sources (AA)
- Identity Providers (IDP)
- Relying Parties (RP)
- Attribute Exchange Network (AXN)
- Proxy
- User
- Key Mgmt
- Audits
- Data Store & Metadata Index
- Labeler
- Policy Service Engine
- Policies
- Decision Service
- ABAC Access Results
- Policy Enforcement Point

RP’s ABAC Infrastructure Overview
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