Online Identity Attribute Exchange
2013 - 2014 Initiatives
Agenda

- Overview
- AXN Services Framework
- ABAC Services
- Demonstration
- Summary
Online Identity Is Broken
Lack of Business, Legal, and Technical Interoperability
• Password re-use degrades security and privacy
• Unknown cross jurisdictional legal risks and liability overhang

$1B+ Opportunity
Affordable + On-Demand + Verified User Attributes = Internet Growth
• Identity verification and interoperability are critical
• Reduce online global legal patchwork and friction/cost

Industry Driven Approach
Increased Use of Trusted Attributes Online with Minimized Friction
• User asserts and permissions binding of verified real world & online identities
• Interoperable technology and legal standards - predictable and enforceable at Internet scale
Efficient Online Identity Ecosystems Drive Market Faster/Further

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

Use of Verified Attributes ➔ Increases Trust ➔ Decreases Friction

Quantitative Trust = ↑ Revenue

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>↑ Speed</td>
<td>Expand Existing Markets</td>
</tr>
<tr>
<td>↓ Costs</td>
<td>Enable New Services</td>
</tr>
<tr>
<td>↓ Risk</td>
<td>Mitigate Fraud</td>
</tr>
<tr>
<td>↑ Transactions</td>
<td>Competitive Differentiation</td>
</tr>
</tbody>
</table>

Qualitative Trust ~ ↑ Brand Value

↑ Perceptions of transparency, security and privacy
Pilot Program Outcome: Implement a user-centric online Identity Ecosystem and demonstrate an Attribute Exchange Trust Framework using the ID Dataweb (IDW) Attribute Exchange Network (AXN)

Project Approach:
• Demonstrate online credential and attribute exchange operations and features of an attribute exchange trust framework
  – User, AP, IdP, and RP interfaces and process/data flows
  – Legal, policy, and technical interoperability, security, and scalability
  – Business and market monetization models
  – Assessor roles and processes

Project Objectives:
• Simplify AP, RP, and IdP participation, deploy new online services and demonstrate asset monetization via the IDW AXN platform using:
  – Real-time AP online verification services
  – Out of band verification services – SMS to device, device IDs, biometric verification services
• Live user data from commercial and government RPs
• RP billing (monthly) and AP/IdP transaction/payment statements
• Commercial contracts and Terms of Service that transition pilots to commercial operations

NSTIC Pilot Use Case Scenarios:
• Basic Use Case scenarios will initially be limited to key identity attributes: Name, e-mail, Address, Telephone Number (NEAT) and sending one-time passwords via SMS to a mobile device
• Increasingly complex and advanced Use Cases will include additional attributes, interoperability between an OpenID or SAML credential, CAC/PIV card credentials, and identity linkage to end-user devices
• For each RP Use Case: Free market trial of verified attribute services for 180 days or 50,000 users, whichever occurs first
Tight Budget with Large Mission and Expanding Scope
- Original schedule to move the AXN Ecosystem in line with NSTIC Principles was aggressive – *disruptive strategy and “crossing the chasm”* with identity federation
- Migration completed to AWS with privacy enhancements

AXN Value Proposition & Community Outreach is Impacting the Ecosystem
- Important lessons learned from early adopter pilots
- Well defined mission and federation use cases
- Short term RP contractual hurtles are nearing conclusion
- 20+ solution providers working to join the AXN and are adapting to AXN privacy and data minimization requirements
- Device ID, Biometrics, ABAC and UMA requirements in 2014 will add more solution providers for advanced use cases

Year 2 Pilots are High Value, Visible and May Enable Trust Frameworks
- Strong federation value propositions for RPs will drive market adoption
- Significant cross pilot collaboration

Continued need for NSTIC and community support
- More RPs and outreach to Communities of Interest
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

© 2013 Criterion Systems, Inc. Proprietary and Confidential
Criterion Systems, Inc. retains ownership of its proprietary information in this presentation.
Federated Identity Use Cases

- **Federated User 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 Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Broadridge Use Case</strong></td>
</tr>
<tr>
<td>Industry: B to C</td>
</tr>
<tr>
<td>RP Service: Fluent – Online Application Platform for Investor Communications</td>
</tr>
</tbody>
</table>

| **Industrial Enterprise Use Case** (Pending Final Approval) |
| Industry: B to C, B to B |
| RP Service: Various Service Sector Applications Corporate, Partner and Consumer Account Access |

| **DHS/FEMA (MIT Lincoln Labs) First Responder Use Case** |
| Industry: G to G, G to C |
| RP Service: Account creation and login for the First USA disaster response collaboration portal |

| **eBay Use Case** |
| Industry: B to C, C to C |
| RP Service: Retail Seller and Buyer Account Creation and Login |
### Year 2 NSTIC Pilots

#### Relying Party Use-Case By Task/Month

<table>
<thead>
<tr>
<th>Year 2 Pilot Project Operations</th>
<th>Year 3 Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess</td>
<td>POC</td>
</tr>
<tr>
<td>10,000</td>
<td>10,000</td>
</tr>
</tbody>
</table>

#### Use-Case RP#5
- **Budget Narrative 2014**: TSCP – Supply Chain
- **Current Plan**: Assess
- **User Verifications**: POC, TSCP – Supply Chain
- **Census**: Assess

#### Use-Case RP#6
- **Budget Narrative 2014**: DFARS Case 2011-D039, technical information must have “data labeling controls” and can only be accessed by approved credentials LOA 2 through LOA 4.
- **Current Plan**: Assess
- **User Verifications**: POC, Contract Activities, POC
- **Census**: Assess

#### Use-Case RP#7
- **Operation**: various consumer-facing sites for consumer account access
- **User Verifications**: POC, Basic Operations, Advanced, Graduate
- **Census**: Assess

#### Use-Case RP#8
- **Operation**: ProxyVote.com
- **User Verifications**: POC, Basic Operations, Advanced, Graduate

#### Relying Partner | Potential Use Cases
---|---
**TSCP – Supply Chain** | DFARS Case 2011-D039, technical information must have “data labeling controls” and can only be accessed by approved credentials LOA 2 through LOA 4.
**Census** | Q2/Q3 2014 Demographic Survey
**Global Industrial Consumer Facing #2** | Various consumer-facing sites for consumer account access
**Broadridge #2** | ProxyVote.com
**Intl. Products & Services Co.** | Supply chain or reseller credential federation
**Health Information Exchange** | Consumer account creation using federated IdP credentials with ABAC (backup)
## IdAM Constituency To Approach

### Source: Gartner Group

<table>
<thead>
<tr>
<th>Life Cycle/Constituency</th>
<th>Employee Services</th>
<th>Contractor Services</th>
<th>Vendor Services</th>
<th>Partner Services</th>
<th>Customer Services</th>
<th>Public Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose/Posture</strong></td>
<td>Enable/Provide/Manage/Collect</td>
<td>Enable/Provide/Manage/Collect</td>
<td>Enable/Manage/Collect</td>
<td>Enable/Provide/Support</td>
<td>Expose/Sell/Service/Provide</td>
<td>Expose/Sell/Service/Provide</td>
</tr>
<tr>
<td><strong>Life Cycle Event/Options</strong></td>
<td>Ent. Admin/Change in Authoritative Source</td>
<td>Delegated Admin/Change in Authoritative or Federated Source</td>
<td>Delegated Admin/Self-service/Federated Provisioning -SCIM</td>
<td>Delegated Admin/Self-service/Federated Provisioning -SCIM</td>
<td>Self Service/Social Identity (OpenID)/Federated Provisioning -SCIM</td>
<td>Self Service/Social Identity (OpenID)/Federated Provisioning -SCIM</td>
</tr>
<tr>
<td><strong>Audit</strong></td>
<td>Access Cert./Reporting</td>
<td>Access Cert./Reporting</td>
<td>Access Cert./Reporting/Real-time Monitoring</td>
<td>Real-time Monitoring/Fraud Detection</td>
<td>Real-time Monitoring/Fraud Detection</td>
<td>Real-time Monitoring/Fraud Detection</td>
</tr>
</tbody>
</table>
AXN Services Framework

Identity Providers (IdP)

Attribute Providers (AP)

Trust Framework Provider (TFP)

Proxy

Attribute Exchange Network (AXN)

Assessors & Auditors

Dispute Resolvers

Relying Parties (RP)

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

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

User Services

- Attributes: Not Stored In AXN, Self Asserted, Data Minimization
- PDS: PII, Preferences, ABAC, Encrypted, External Store

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

Criterion Systems, Inc. retains ownership of its proprietary information in this presentation.
### AXN Providers and Roles as of 12/31/13

<table>
<thead>
<tr>
<th>Role</th>
<th>Provider on the Exchange</th>
<th>Description of Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity Providers</strong></td>
<td>LOA3+: Lockheed Martin, Raytheon, Boeing, Verizon, Symantec*</td>
<td>Credential Authentication Services</td>
</tr>
<tr>
<td></td>
<td>LOA 1: Google, AOL, Facebook, Linkedin*, Amazon*, Salesforce</td>
<td></td>
</tr>
<tr>
<td><strong>Attribute Providers</strong> (PII Verification)</td>
<td>Experian, LexisNexis, Pacific East, Enterprise LDAP/Directories*, Equifax*, Thomson Reuters*</td>
<td>Traditional validation of user PII (Name Address, Telephone, BOD, and Social)</td>
</tr>
<tr>
<td><strong>Device ID</strong></td>
<td>Telesign, Wave, Payfone*</td>
<td>Identification of the access device via the PIN, TPM chip, software download, or other means</td>
</tr>
<tr>
<td><strong>BIO metrics</strong></td>
<td>Daon, CGI*</td>
<td>Service are capable of voice, face and other like recognitions at varying degrees of sophistication.</td>
</tr>
<tr>
<td><strong>Signature/ Key Stroke Dynamics</strong></td>
<td>Kaje, Autheware*</td>
<td>Alternative signature capture</td>
</tr>
<tr>
<td><strong>Document Proofing</strong></td>
<td>ID Checker*, Experian*</td>
<td>Confirms the government issued document is legitimate and matches the user PII</td>
</tr>
</tbody>
</table>

* We have not finalized testing the integration of this service.
**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
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)** [http://invis.io/NYN0E4JZ](http://invis.io/NYN0E4JZ)
  – 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
AXN - ABAC Ecosystem

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

RP’s ABAC Infrastructure:

- **Data**
- **ABAC Access Results**
- **Attribute Service Input**
General Lessons Learned

- RPs are the customer, and will drive market requirements, adoption, and policy controls.
- Online retailers may not be early adopters of login with federated credentials due to concerns about user drop off rates; will likely be strong adopters as federation matures.
- 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.
- Current IdP and RP business practices do not always conform to FIPP’s, and need to be managed.
- A rigorous Privacy Evaluation Methodology (PEM) implementation resulted in significant benefits
  - 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.
Contractual Lessons Learned

• Traditional AP compliance policies have been modified to support products that DO NOT provide PII back to the AXN. Items we have negotiated
  – Out of the AP contracts:
    – System security requirements for RPs
    – Auditing of RPs systems and records for PII usage
  – In the AP contracts:
    – Knowledge of the RPs is mandatory for the APs, however the user’s relationship with the RP will be kept private

• Consolidating the terms of dozens of contracts and lawyer communities into a single agreement for the AXN has proven to be challenging
  – Consider an 80% solution where specific products used by the RP have their own unique addendums even if there are overlaps
  – Trust Framework providers will likely influence the contracting process
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