NISTIC Pilot - Attribute Exchange Network
Biometric Consortium Conference - 2013
Market Development

**Startup (2011)**
- Unrealized Large Market Potential
- Evolving Value Props & Use-Cases
- Evolving Tech/Policy Standards
- Initial Tech Implementations
- Low Volume Pricing (inefficient)
- Disruptive Tech/Business Models

**Pilots/Early Adoption (2012)**
- Unproven Market
- Defined Market Objectives & Metrics
- Baseline Tech/Policy Standards
- Demo and Pilot Systems Ready
- Low Volume Pricing (inefficient)
- Contracts w/Early Participants

**Growth/Efficient (2013 +)**
- Established Market Adoption
- Expanding Portfolio of Use-Cases
- Stabilized Tech/Policy Standards
- Technology – Proven & Operational
- High Volume Pricing (efficient)
- IdP, RP, AP and AXN Market Evolution

**Proforma “Street Identity” Market Adoption**

**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

© 2013 Criterion Systems, Inc. Proprietary and Confidential
Criterion Systems, Inc. retains ownership of its proprietary information in this presentation.
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 communications and/or 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
Enabling IT & Other Values

• Cloud implementation
  – Real-time information verification services
  – Authoritative information sources
• Reduce account creation and maintenance costs
  – Customer single sign on using a known login to reduce drop off
  – Credential Federation – verified attributes are used to create new or bind to existing user accounts
• Additional signals including
  – Strength of authentication credentials
  – Adaptive access (“step up”) verification and authentication methods for high risk or sensitive transactions
• Select appropriate attribute sources based on
  – Confidence level
  – Price point
  – Tiered verification mechanisms to enable broad (global) coverage
• Select information sets to meet the needs of specific transaction types (FIPPS data minimization)
## IdAM Constituency To Approach

### Life Cycle/Constituency

<table>
<thead>
<tr>
<th>Purpose/Posture</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>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>
<td></td>
</tr>
</tbody>
</table>

### Life Cycle Event/Options

<table>
<thead>
<tr>
<th>ID Store</th>
<th>Authorization</th>
<th>Authentication</th>
<th>Audit</th>
</tr>
</thead>
<tbody>
<tr>
<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>
</tr>
<tr>
<td>Federated Enterprise Directory</td>
<td>Roles/Rules/ABAC</td>
<td>Username/Pswd/Strong Auth/Federate/ID Proofing</td>
<td>Access Cert./Reporting</td>
</tr>
<tr>
<td>Federated Enterprise Directory</td>
<td>Roles/Rules/ABAC</td>
<td>Username/Pswd/Strong Auth/Federate/Adaptive Access/ID Proofing</td>
<td>Access Cert./Reporting</td>
</tr>
<tr>
<td>Federated Enterprise Directory/VDS</td>
<td>Roles/Rules/ABAC</td>
<td>Username/Pswd/Strong Auth/Federate/Adaptive Access/ID Proofing</td>
<td>Access Cert./Reporting</td>
</tr>
<tr>
<td>Federated Enterprise Directory/VDS</td>
<td>Roles/Rules/ABAC</td>
<td>Username/Pswd/Strong Auth/Federate/Adaptive Access/ID Proofing</td>
<td>Access Cert./Reporting</td>
</tr>
<tr>
<td>Federated Enterprise Directory/VDS</td>
<td>Roles/Rules/ABAC</td>
<td>Username/Pswd/Strong Auth/Federate/Adaptive Access/ID Proofing</td>
<td>Access Cert./Reporting</td>
</tr>
<tr>
<td>Federated Enterprise Directory/VDS</td>
<td>Roles/Rules/ABAC</td>
<td>Username/Pswd/Strong Auth/Federate/Adaptive Access/ID Proofing</td>
<td>Access Cert./Reporting</td>
</tr>
<tr>
<td>Federated Enterprise Directory/VDS</td>
<td>Roles/Rules/ABAC</td>
<td>Username/Pswd/Strong Auth/Federate/Adaptive Access/ID Proofing</td>
<td>Access Cert./Reporting</td>
</tr>
<tr>
<td>Federated Enterprise Directory/VDS</td>
<td>Roles/Rules/ABAC</td>
<td>Username/Pswd/Strong Auth/Federate/Adaptive Access/ID Proofing</td>
<td>Access Cert./Reporting</td>
</tr>
</tbody>
</table>

### Source:
Gartner Group
AXN Services Framework

Identity Providers (IdP)
- 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)
- Attributes: NEAT, SS, DOB, Gender, Corp Verification
- Quality: Refresh Rate, Coverage, Sources, Data Types
- Physical: Device ID, BIO, Card, Other
- Pricing: Per Transaction, Per User, Per Year, Annual License
- Cert/TF: FICAM, OIX, Kantara, Other

Trust Framework Provider (TFP)

Proxy

Attribute Exchange Network (AXN)
- AP Services
- Attributes: NEAT, SS, DOB, Gender, Corp Verification
- Quality: Refresh Rate, Coverage, Sources, Data Types
- Physical: Device ID, BIO, Card, Other
- Pricing: Per Transaction, Per User, Per Year, Annual License
- Cert/TF: FICAM, OIX, Kantara, Other

Assessors & Auditors

Dispute Resolvers

Relying Parties (RP)
- RP Services
- Enroll: Business Purpose, Attribute Selection, Claims Refresh Rate, IdP & RP Selections, User Preferences, Contract
- LOA: LOA 1-4
- Admin: Logs, Reporting, Billing, Contract Management
- 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
1. **Credential Federation**
   - Verified attributes are used *to create new or bind to existing* user accounts

2. **Personal Data Services (PDS)**
   - User attribute data is not stored in the AXN
   - PDS data is presented via MAX to create and manage RP accounts
   - User-centric, privacy protective, secure, and *federated*
   - No cost to user

3. **User Managed Admin (UMA) Console**
   - Authenticated users have federated access at each RP
   - Created when a user first opts in to share their verified attribute claims via the AXN with an RP
   - Users can securely manage PDS attributes shared with an RP service accessed by an IdP credential
   - Enables user to link and unlink multiple IdP credentials
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 Privacy – By Design

- AXN legal agreements
  - Standardized agreements with regulatory flow down terms from IdPs and APs
  - Limit PII collection to what is necessary to accomplish the specified purpose(s)
  - Accountability and audit to protect PII through appropriate safeguards
- AXN as a proxy - no single service provider can gain a complete picture of a user’s activity
- The AXN data management design mitigates potential threats
  - Does not create a central data store of verified user attributes
  - Security and privacy enhancing technology is built into the AXN infrastructure
- Users opt-in to each control process for collection, verification, and distribution of attributes
  - User Admin console for attribute and credential management
  - Only the minimum necessary information is shared in a transaction (FIPPS)
# The First Year NSTIC Use Cases

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

<table>
<thead>
<tr>
<th>Industry</th>
<th>Industrial Enterprise Use Case (Pending Final Approval)</th>
</tr>
</thead>
<tbody>
<tr>
<td>B to C, B to B</td>
<td>RP Service: Various Service Sector Applications Corporate, Partner and Consumer Account Access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry</th>
<th>DHS/FEMA (MIT Lincoln Labs) First Responder Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>G to G, G to C</td>
<td>RP Service: Account creation and login for the First USA disaster response collaboration portal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Industry</th>
<th>eBay Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>B to C, C to C</td>
<td>RP Service: Retail Seller and Buyer Account Creation and Login</td>
</tr>
</tbody>
</table>
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.
- 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.