Attribute Exchange Trust Framework Specification

DRAFT Technical Specification v 1.0

Document Version: 1.0 Serial No.

Date: 2 July 2013

Terms and Conditions

This specification was developed and is being released under this open source license by Open Identity Exchange (OIX).

Use of this specification is subject to the disclaimers and limitations described below. By using this specification you (the user) agree to and accept the following terms and conditions:

1. This specification may not be modified in any way. In particular, no rights are granted to alter, transform, create derivative works from, or otherwise modify this specification. Redistribution and use of this specification, without modification, is permitted provided that the following conditions are met:

- Redistributions of this specification must retain the above copyright notice, this list of conditions, and all terms and conditions contained herein.
- Redistributions in conjunction with any product or service must reproduce the above copyright notice, this list of conditions, and all terms and conditions contained herein in the documentation and/or other materials provided with the distribution of the product or service.
- OIX's name may not be used to endorse or promote products or services derived from this specification without specific prior written permission.

2. The use of technology described in or implemented in accordance with this specification may be subject to regulatory controls under the laws and regulations of various jurisdictions. The user bears sole responsibility for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such laws or regulations.

3. THIS SPECIFICATION IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. OIXAND EACH OIX MEMBER DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, QUIET ENJOYMENT, ACCURACY, AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER OIX NOR ANY OIX MEMBER WARRANTS (A) THAT THIS SPECIFICATION IS COMPLETE OR WITHOUT ERRORS, (B) THE SUITABILITY FOR USE IN ANY JURISDICTION OF ANY PRODUCT OR SERVICE WHOSE DESIGN IS BASED IN WHOLE OR IN PART ON THIS SPECIFICATION, OR (C) THE SUITABILITY OF ANY PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF OIX OR ANY THIRD PARTY.

4. IN NO EVENT SHALL OIX OR ANY OIX MEMBER BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS SPECIFICATION, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S OR OIX MEMBER'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS SPECIFICATION, THE USER WAIVES ANY SUCH CLAIM AGAINST OIX OR ANY OIX MEMBER RELATING TO THE USE OF THIS SPECIFICATION. IN NO EVENT SHALL OIX OR ANY OIX MEMBER BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO ANY USER OF THIS SPECIFICATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. OIX reserves the right to modify or amend this specification at any time, with or without notice to the user, and in its sole discretion. The user is solely responsible for determining whether this specification has been superseded by a later version or a different specification.

6. These terms and conditions will be interpreted and governed by the laws of the State of _____ without regard to its conflict of laws rules. Any party asserting any claims related to this specification irrevocably consents to the personal jurisdiction of the U.S. District Court for the _____ and to any state court located in such district of the State of _____ and waive any objections to the venue of such courts

Document Change History For: OIX AXWG v1 - AXTF Specification

Version Number	Version Date	Information Affected	Author(s)	Authorized by
0.1	10 December 2012	First Draft	David Coxe	OIX AXWG Project Team
.2	27 March 2013	Privacy Section	Dale Rickards, Rich Furr	OIX AXWG Project Team
.3	3 May 2013	Assessor/Certification Section	Sal D'Agostino, Myisha Frazier-Mcelveen	OIX AXWG Project Team
.4	16 May 2013	Second Draft	David Coxe	OIX AXWG Project Team
.5	10 June 2013	Final Draft	David Coxe	OIX AXWG Project Team
.5.1	21 June 2013	Insertion of TIG as a new Appendix	Scott Rice	
.6.0	23 June 2013	Summary & Conclusions	David Coxe	
.6.1	25 June 2013	Final Edits	David Coxe John O'Brien	OIX AXWG Project Team
.7.0	2 July 2013	Final Edits part 2	David Coxe John O'Brien	OIX AXWG Project Team

Document Contributors

Member Name	Member Company
David Coxe	ID Dataweb
Peter Graham	Verizon
Kim Little	LexisNexis
Tom Smedinghoff	Edwards Wildman Palmer LLP
John Bradley	Ping Identity
Scott Rice	Pacific East
Mike Leszcz	Pacific East
Pam Dingle	Ping Identity
Dale Rickards	Verizon
Myisha Frazier-McElveen	Deloitte & Touche
Ray Kimble	Deloitte & Touche
John Dials	ID Dataweb
Chris Donovan	ID Dataweb
Domenic DiLullo	Accenture (formerly Department of Homeland Security)
Bob Coxe	ID Dataweb
Sal D'Agostino	ID Machines
Andrew Nash	Individual Contributor
Naomi Lefkovitz	NIST, NSTIC Senior Privacy Advisor
Don Thibeau	OIX
John E. O'Brien	Verizon

TABLE OF CONTENTS

TABLE OF FIGURES

Introduction

Background

Affordable, private and secure access to online services is linked to broader and better use of the Internet and global economic growth. However, today most Internet services know little more about you than that you are an email address. This limits the set of services that can be offered to consumers. With the addition of information such as home address or mobile phone number a wider range of service providers are able to certify that your email address is linked to the real world individual that they often already know about. So a utility provider can ascertain that your identity provider is representing the correct customer, the media company can verify that you have access to premium content, or the health care provider can connect you to your lab test results. In all of these cases we assume that the user is engaged in the exchange of information so they may provide permission for identifying information to be shared with a service provider from an attribute provider.

Building online trust may involve individuals using an email or social (or other) identity provider – both public and private – to authenticate themselves online for different types of transactions. Online trust may also require the Internet identity ecosystem to be user-centric – that means each of us, as a user, would have more control of the private information we use to authenticate ourselves on-line, and generally would not have to reveal more than necessary.

A person's real world physical attributes or identifiers are used to help link their online logical identifiers to authenticate that individual's identity when rendering a service. For example, many organizations currently use postal mailers as a low cost, high scale, identity-proofing process to validate the link between a logical address (email) and a physical address (postal mail). Improving today's process through increased speed and security will allow offline data repositories (such as the NIH, Social Security, VA, IRS, banks and various telephone databases) to link the physical address to a physical identity.

This linkage improves the identity vetting process for online identities (identifier + address + other attributes such as name, gender, age, depending on requirements). It also allows individuals to share information about themselves from a variety of attribute providers that results in a more significant set of interactions with service providers on the Internet. These identity information services will greatly enhance online transaction trust and security consistent with the goals of the National Strategy for Trusted Identities in Cyberspace (NSTIC) and similar programs in other nations.

Intent

The intent of the Attribute Exchange (AX) Trust Framework specification is to enable what some call the "Identity Information Exchange Ecosystem." This is an ecosystem or marketplace that is interoperable, secure, and allows users to share reliable identity information with service providers who wish to utilize them. The objective is to provide a starting point from which a Community of Interest (COI) can organize participation from their constituency to customize and implement the business, legal, technical, privacy, certification and audit components of their AX Trust Framework specification.

As defined herein, an Attribute Exchange Trust Framework is designed to enable trusted delivery of online services to users with a scalable, secure, low-cost, and convenient solution. A framework consists of multiple parties whereby a user is issued a digital credential by a commercial identity provider (IDP), such as their bank, email or social network provider, with which they already have an online relationship. This credential is used to interact online with a service provider called a Relying Party (RP). RPs may in turn request additional information about a user that is satisfied by Attribute Providers (AP) that are granted access rights by users.

Agreements between all parties contractually enforce the business, legal, technology, policy, certification and audit aspects of the Trust Framework, which are established and managed by a Trust Framework Provider (TFP) via an Attribute Exchange Network (AXN). When adopted across a broad range of IDPs and RP websites and applications, the Attribute Exchange Trust Framework provides a scalable solution for online user attribute

exchange to enable higher levels of assurance, authentication and authorization at a lower cost and with greater convenience for users.

To support these objectives, the AX Trust Framework will specify a consistent, provider-agnostic set of information exchange protocols and policies for the purpose of facilitating attribute verification, digital identity management and fraud prevention. These information exchange protocols and policies, or "rules and tools", would allow for access to necessary user identity attributes as requested by an RP for a specific transaction without interfering in, risking, or devaluing the primary relationship between the user and the online community of RPs.

More specifically, the AX Trust Framework will embrace the following principles:

- Enhance online privacy and trust by referencing and encouraging parties to follow the Fair Information Practice Principles (FIPPs) (in the US or other data minimization policies as appropriate), and allow participants to "opt-in" or opt-out with their shared information.
- Provide secure and reliable methods of exchanging user-asserted and verified attributes for online electronic account creation using "out of band methods" or by a community of attribute providers who meet the necessary requirements to verify the identity attributes of online users. The use of these attributes by service providers could also be effectively revoked or suspended by the individual user in instances of misuse.
- Support identity portability and interoperability by enabling participants to assert their digital identities to RPs by implementing cost-effective and easy to use open standards such as OAuth 2.0, UMA, SCIM, SAML, OpenID, and OpenID Connect to solve a robust set of business requirements.
- Reduce online transactions costs by eliminating redundant account procedures and reducing fraud.
- Enable the commercial and government service providers to expand their online services in order to serve its constituents with increased efficiency and transparency.
- Enable protocols and policies for verifying, handling and exchanging user-asserted attributes that avoid organizational conflicts of interest that would compromise user trust in the ecosystem of participants.
- Provide for an audit and certification process that ensures any entity with access to user-asserted and verified attributes uses it only for the purposes allowed and accepts and follows the limitations placed on the data and services by the user, the RP or the appropriate regulatory authority.

Attribute Exchange Networks

An Attribute Exchange Network (AXN) is an online Internet-scale gateway for IDPs and RPs to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs. The AXN standards-based platform deploys a business model that simplifies online identity verification for APs, RPs, and IDPs. This business model will ultimately reduce costs to RPs while generating revenue to APs and IDPs. The user is issued a login credential (e.g., OpenID, SAML) by an IDP, such as a government agency, bank, e-mail or social network provider with whom they have an established online relationship. This digital credential is recognized and accepted within the network of framework participants and used in lieu of creating a new user name and password to interact online with each RP service provider. RPs, at their discretion, will pay to verify additional user identity attribute claims such as full name, street address, phone number, or age to satisfy the RP's security requirements for reducing risk. In the case of high security, high value or risky transactions, the AXN will support various trust elevation methods including interoperability between an OpenID or SAML credential, Personal Identity Verification (PIV) Interoperability (PIV-I), Common Access Card (CAC) credentials, and identity linkage to end-user devices (e.g., laptops and mobile phones). The user is not charged to participate; the RP pays less than what they currently pay to validate user attributes; and IDPs and APs increase their revenue.

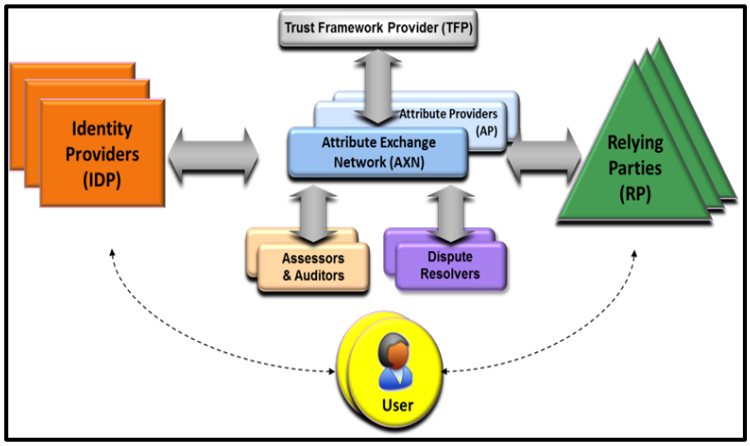


Figure 1: Identity Attribute Exchange Ecosystem

As shown in Figure 1, the AXN enables this Identity Ecosystem by providing a common API gateway that allows RPs, IDPs, and APs to interact using a one-to-many relationship model that reduces barriers to entry in the Identity Ecosystem.

The AXN's revenue model is based on a mutually beneficial business model, the composition and commitment of the existing industry participants, and the availability of public and private sector RPs. The AXN business model is critical to overcoming historical implementation barriers and expanding the participation of RPs through a mechanism for efficiently servicing and monetizing existing RP markets and new business currently underserved by the existing online Identity Ecosystems.

The AXN also provides a means for APs to efficiently access and monetize their AP services to a large array of IDPs and RPs in global online markets. The AXN is responsible for the processes and policies associated with establishing, maintaining, and distributing verified user identity attributes. AXN attribute maintenance includes validating, updating, and revoking attribute claims. An attribute provider on the AXN validates a user-asserted attribute claim and the AXN provisions that verified claim, with user permission, in response to attribute requests from RPs.

AXN AP participants use the standards-based APIs and cloud-based, interoperable transaction AXN infrastructure to share revenue generated from RPs for purchases of verified user-asserted attributes. The AXN promotes user trust, security, and privacy by participating in auditable trust framework processes and policies, as exemplified by OIX. The AXN also expands the addressable market not currently supported by APs to include small and medium size RPs by enabling affordable access to verified user attributes via an online attribute exchange.

The AXN will raise the level of confidence across the Identity Ecosystem by enabling the following services:

- Manage secure, one-to-many open standards-based APIs to connect all participants to the AXN infrastructure platform for data flows between APs, IDPs, and RPs
- Manage payment collections from RPs for verified attributes and distribute payments to APs and IDPs
- Manage standard legal contracts and appropriate Service Agreements (SAs) for attribute exchange on a one-to-many basis with IDPs, RPs, APs, and Trust Framework Providers (TFP), Assessors, and user Terms of Service (TOS)
- Support a user attribute management interface to enable user attribute opt-in/opt-out for each RP account relationship through an AXN user Admin Console, or support this service through the user's IDP
- Support policy compliance by ensuring the AXN collection, storage, release, transport, and use of user attributes with APs, IDPs, and RPs channels conforms with Trust Framework business, legal, technical, and privacy policy controls
- Manage transaction logs with AP, IDP, and RP channels in support of ongoing security, privacy and policy audit requirements as defined for each trust framework

The AXN reference architecture enhances user privacy and control over their verified user attributes without creating a centralized data store of user attributes at the AXN. Throughout this identity ecosystem, the user will be leveraging a credential (e.g., OpenID) issued and managed by their IDP, which minimizes the use of passwords and reduces the friction associated with user account creation and log in.

Attribute Exchange Trust Frameworks

Trust frameworks increase the use of identity data online with minimal stakeholder conflict that enables the trusted use of verified attribute claims to support higher levels of assurance (LOA) for online transactions. Trust frameworks are based on open technology and legal standards that enable reliable, predictable, and enforceable standards. They provide an identity network where voluntary standards benefit all participants.

This specification of the "rules and tools" for building trust in online identity via an Attribute Exchange (AX) Trust Framework takes on new importance and urgency given the increasing deployment of new products and services amid decreasing levels of Internet security and user privacy. Once this specification is approved, it can be published for open use, customization, and implementation by industry specific Trust Framework Providers.

Parties who wish to obtain or verify user identity attributes may include Relying Parties and Identity Service Providers who are willing to comply with the rules, limitations and data protections specified in an Attribute Exchange Trust Framework for their community of interest. Members of an Attribute Exchange Trust Framework will supply these rules to Open Identity Exchange (OIX) which can facilitate audits of members, utilizing

independent "Assessors" to ensure Trust Framework members and parties who rely on their services are abiding by the rules that are established. The components of such a framework must include:

- A description of one or more service definitions that specify a means and protocol for attribute exchange, the data necessary to initiate the attribute exchanges and the information returned
- Documentation of the "Levels of Protection" a given service must afford the identity provider
- Documentation of the "Levels of Assurance" a given service provides the entity relying upon the service
- Documentation of the "Levels of Control" afforded the party or entity about whom the attribute exchange references.

At a minimum, a trust framework related to attribute data exchange should provide for the following components:

Policy Components (Rules):

- Definitions (User, Identity Service Provider, Attribute Provider, Assessors, Attribute Exchange Network, Relying Party, Trust Framework Provider, etc.)
- Permissible uses of user data (for example, for attribute verification, fraud prevention and identity authentication) and possible indexing to existing regulation sets
- Data retention rules and policies
- Rules for avoiding organizational conflicts of interest
- Audit elements and procedures
- Certification requirements and service marketing restrictions
- Stratification of information exchange protocols into appropriate standards for Levels of Assurance
- Broad attribute use (emphasize "use" of attributes consistent with ALL stakeholder rights and interests)
- "Unpack" existing identity system function and values to identify new markets and user control opportunities
- Broad focus on provisioning of new attribute based services to relying parties and data subjects in systems
- Identification of metrics that correlate to new value propositions

Technical Components (Tools):

- Supported transactions and transaction standards
- Supported information exchange protocols (for example OpenID Connect, Oauth 2.0, UMA, SCIM or XML)
- User permissions and categories of permissions (for example, the framework might provide the means for a user to opt-in to allow commercial transaction to be authorized, but perhaps not allow users to opt-out of fraud prevention)
- The Trust Framework scope, development and implementation will be limited to the first 3 steps of the 5 Steps of Trust Framework Rule Making:
    1. "Agenda Setting" (broad attribute-related services focus)
    2. "Problem Identification" (helping to design pilots and other "experiments" to test system proposals)
    3. "Decision"
    4. "Implementation"
    5. "Evaluation" (need for stakeholder critique to fully evaluate and evolve ideas of pilots into scalable systems)

The Implementation and Evaluation steps (4 and 5) will be conducted by a community of interest (COI) via separate project initiatives, and ultimately through the implementation of a trust framework by independent Trust Framework Providers who customize the OIX Attribute Exchange Trust Framework to suit the business purposes of a specific business or government community of interest.

Deploying An Attribute Exchange Trust Framework

While the overall objectives of an AX Trust Framework will include improving online user trust, privacy, and online security, the intent of the OIX Attribute Exchange Trust Framework specification is to publish a practical roadmap for how a TFP can quickly implement a trust framework to address their specific market requirements. RP Use Cases and an AXN reference architecture serve as the common foundation for the work group contributions included in this AX Trust Framework specification. The OIX AX Trust Framework Specification contained herein is a starting point from which each Community of Interest (COI) will need to organize participation from their constituency to customize the business, legal, technical, privacy, certification and audit components of their AX Trust Framework specification.

The COI **Business Group** should lead this effort by identifying industry sectors ideally suited for an AX Trust Framework and developing RP Use Cases, service definitions, monetization models, and high level requirements related to business, legal, and technical processes. Additionally, various Use Case models must be defined for establishing a TFP business entity for exchanging ownership, obtaining resources, and securing funding from industry participants and to define ongoing income streams to perpetuate trust framework operational requirements.

The COI **Legal Group** should deliver the legal portion of the AX Trust Framework Specification. As the AX Trust Framework specification evolves, a set of legally binding agreements should be implemented based on a common set of criteria to manage risk with the AXN serving as a contractual hub. The objective should be to deliver a set of legal agreements that are required to implement an active trust framework.

The COI **Technology Group** should deliver the technology, standards, data flows, and technical interface criteria for the AX Trust Framework specification based on the AXN reference architecture. Below is a high level list of topics that should be covered by the working group.

- Identify supported transactions and transaction standards
- Identify supported information exchange protocols (e.g., OpenID, OpenID Connect, OAuth, SCIM, XML)
- Identify supported technical interoperability standards (e.g., OpenID, XUA, UMA, SAML, PKI)
- Identify supported APIs
- Develop models for data flows, data handling, and data caching

The COI **Privacy Policy Group** should be responsible for ensuring the Internet Identity Ecosystem is user-centric, meaning each individual user will have more control over the private information used to authenticate themselves online, and generally will not have to reveal more identity data than necessary to use the RP service. This Group should, at a minimum:

- Identify the user permissions and categories of permissions. For example, the trust framework may provide the means for a user to opt-in to allow commercial transactions to be authorized, but perhaps not allow users to opt-out of fraud prevention techniques
- Identify the minimum privacy requirements that should be implement to provide protection for Personal Identifiable Information (PII) exchanged in the AXN.

The COI **Certification/Assessment Group** should be responsible for defining Assessor processes and qualifications, the certification requirements for trust framework membership, and the process for membership recertification. In general, an Assessor must provide written evidence that performing audits is a regular ongoing business activity, including tax filings showing a relevant industry code, financial statements showing a majority of revenue from compliance auditing, and a list of compliance audits performed in the past two years with contact information for verification.

The OIX Attribute Exchange Trust Framework Specification

Introduction

Imagine a world where individuals can conduct sensitive business transactions online with reduced fear of identity theft or fraud and without the need to manage scores of usernames and passwords. In this world, organizations efficiently conduct business online by trusting the identities and credentials provided by other entities. Redundant processes associated with managing, authenticating, authorizing, and validating identity data are eliminated. Loss due to fraud or data theft is reduced and additional services previously deemed too risky are conducted online. Personal information is managed by the individual after it is released to service providers. They are free to use an Identity Ecosystem credential of their choice, provided the credential meets the minimum risk requirements of the relying party. Individuals' participation in the Identity Ecosystem is a day-to-day—or even a transaction-to-transaction—choice.

The identity solutions are scalable across multiple communities, spanning traditional geographic borders. They are interoperable to allow organizations to accept and trust external users authenticated by a third party. They achieve scalability when all participants in the various identity federations agree upon a common set of standards, requirements, and accountability mechanisms for securely exchanging digital identity information, resulting in authentication across identity federations.

The OIX AX Trust Framework Specification contained herein is a starting point from which each Community of Interest (COI) will need to organize participation from their constituency to customize the business, legal, technical, privacy, certification and audit components of their AX Trust Framework specification.

Specification Development: The OIX AX Working Group

Work on this AX Trust Framework Specification commenced in January 2012 with the development of a Working Group and a Charter by participants from the Open Identity Exchange community (Figure 2). The name of the Working Group was the Internet Identity Attribute Exchange Working Group (AXWG), and it was open to all OIX Members and Contributors as defined in the OIX Member Rules.

Figure 2: AXWG Founding Members & Sub-Group Leadership

AXWG was organized and led by OIX membership in response to a growing set of requirements for enabling online trust throughout the identity ecosystem. Participation by a broad variety of stakeholders was strongly encouraged, and community participation included stakeholder representation from:

- Relying Parties: .govs, .edus, and .coms
- Identity Providers: internet (email) (e.g., Google, AOL, etc.) and telco (e.g., Verizon, AT&T, etc.)
- Attribute Providers: (e.g., LexisNexis, Experian, Equifax, PacificEast, Trulioo, etc.)
- Auditors/Assessors: Deloitte, KPMG, etc.
- Standards Organizations: OpenID Foundation, OASIS TEC, Kantara, IDESG, etc.
- Policy Makers: regulators, lawyers & legislators
- End Users: citizens, constituents, and customers; Center for Democracy & Technology
- Trust Framework Providers: (e.g., InCommon, FICAM, OIX)
- Government, commercial, academic entities and others

The purpose of this Working Group was to develop and post an OIX Attribute Exchange Trust Framework Specification to the OIX website. (Figure 3) The initial deliverable included:

- A Working Group Charter accepted by the OIX Board.
- OIX Attribute Exchange Trust Framework Specification, according to the OIX Trust Framework Requirements and Guidelines.
- Acknowledgement of Principles of Openness for the above—a self-assessment of the accountability, transparency, open competition and other characteristics as required by the OIX Trust Framework Listing Agreement.

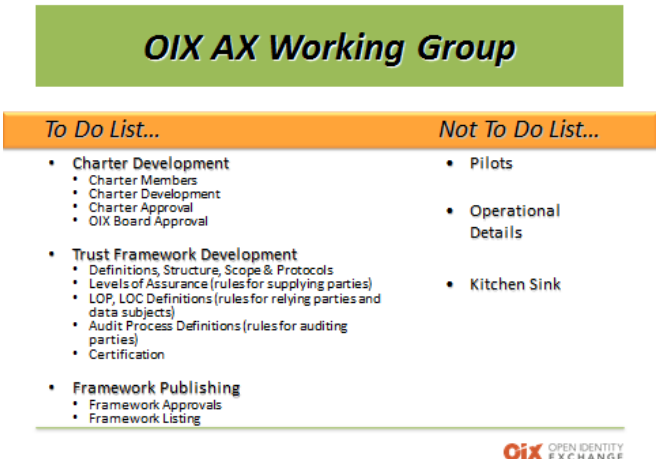


Figure 3: OIX AX Working Group

Items excluded from this work included pilots, operational details and specific implementation requirements for communities of interest. In this context, the purpose of a Trust Framework was to enable 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. In general, a Trust Framework was defined as the tools, rules and business policies that enable assurance for a given community of interest.

The AXWG work groups (Figure 4) formed and were led by industry participants to develop the business, legal, technical, privacy policy and certification/assessor components of the AX Trust Framework specification. Each work group defined a list of objectives with work group charters and scheduled milestones for those deliverables. An Attribute Exchange Network reference architecture and business model was used as the operational context for the Attribute

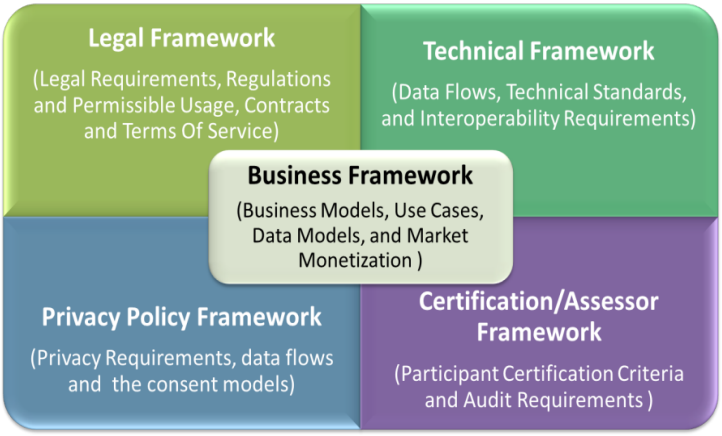


Figure 4: AXWG Work Group Framework

Exchange Trust Framework development (Figure 5). This reference model was used by AXWG participants to develop common language, reference models and interoperability efficiencies while maintaining the dynamic inherent in independent and open community perspectives.

While pilot projects were specifically excluded from the AXWG Charter and work product, AXWG members were actively involved with pilot projects concurrently with the development of the AX Trust Framework specification. As a result, the pilots provided operational context, feedback, and input that was incorporated into the AX Trust Framework specification. Ideally, this AX Trust Framework specification would become a "living" document that would be updated, enhanced and altered to support the requirements of communities of interest over the lifecycle of a portfolio of operational AX Trust Frameworks.

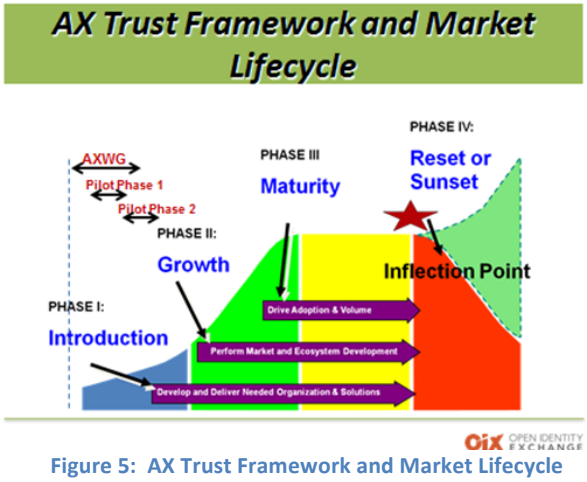


Figure 5: AX Trust Framework and Market Lifecycle

AX Business Framework

Identity management is a foundational issue for most e-commerce transactions and other online activities. Verifying the identity of remote parties, such as determining who is seeking access to an online database of sensitive information, who is trying to do an online transfer of funds from an account, who signed an electronic contract, who remotely authorized a shipment of product, or who sent an email, is a fundamental concern. While participants in many low-risk online transactions are willing to trust that they are dealing with a specific person or entity, as the sensitivity or value of the transaction increases, the importance of ensuring the availability and reliability of accurate information about the identity of the remote party in order to make a trust-based decision increases as well.

The AXN standards-based platform deploys a business model that simplifies online identity verification for APs, RPs, and IDPs. This business model will ultimately reduce cost to RPs while generating revenue to APs and IDPs. The AXN is an online Internet-scale gateway for IDPs and RPs to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs. The user is issued an OpenID credential by an IDP, such as a government agency, bank, e-mail or social network provider with whom they have an established online relationship. This digital credential is used in lieu of creating a new user name and password to interact online a subsequent RP service provider. RP service providers will pay to verify additional user identity attribute claims such as full name, street address, phone number, or age to satisfy RP security requirements and to reduce risk. The user is not charged to participate; RP pays less than what they currently pay to verify user attributes; and IDPs and APs increase their revenues.

The AXN enables this Identity Ecosystem by providing a common API gateway that allows RPs, IDPs, and APs to interact using a one-to-many relationship model that reduces barriers to entry in the Identity Ecosystem. The AXN unique revenue model is based on a mutually beneficial business model, the composition of IDPs and APs on the AXN, and the availability of public and private sector RPs who wish to participate. The AXN business model is critical to overcoming historical implementation barriers and expanding the participation of RPs through a mechanism for efficiently servicing and monetizing existing RP markets and new business currently underserved by the online Identity Ecosystem.

Participants of the OIX AXWG Business Group

- LexisNexis – Kimberly Little
- LexisNexis - Kimberly White
- American Psychological Association – Eva Winer
- Continuum Labs - Bill Nelson
- Edwards Wildman Palmer LLP - Tom Smedinghoff
- Equifax – Pat Mangiacotti
- Experian – Dan Elvester
- ID Analytics – Ken Meiser
- ID DataWeb - Dave Coxe
- OIX - Don Thibeau
- Pacific East – Mike Leszcz and Scott Rice
- Trulioo – Tanis Jorge, Stephen Ufford
- Andrew Nash – individual contributor
- UnboundID - Trey Drake and Nicholas Crown

AX Trust Framework Implementation Checklist

For a community of interest to implement an AX Trust Framework, it is important to start with the industry sectors that have Use Cases that can derive significant benefits by leveraging an AXN (Figure 6). Use Case models must be defined for establishing a TFP business entity for exchanging ownership, obtaining

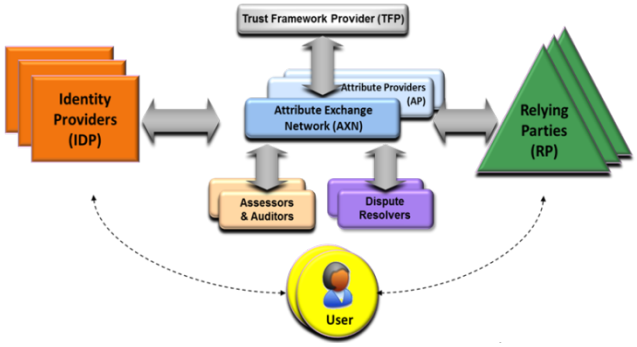


Figure 6: AX Trust Framework

resources, securing funding from industry participants, and to define ongoing income streams to perpetuate trust framework operational requirements.

More specifically, the business checklist of AX Trust Framework implementation tasks includes the following:

1. Identify industry sectors ideally suited for an Attribute Exchange (AX) Trust Framework (TF)
2. Develop TF use-cases, services and requirements (business, legal, technical, privacy/policy, assessor/certification)
3. Identify appropriate data (attribute nomenclature) standards and data sources (authoritative, 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 based on finalized AX Trust Framework Specification
9. Engage in AX pilots at this stage as appropriate
10. Implement AX production operations

Attribute Exchange Market Motivators

Since 2005, eCommerce as a percentage of total retail transactions has been growing steadily at the rate of 8% per year. During 2012, time spent at social networking sites surpassed time spent at portal sites, public cloud services were forecast to grow at 19% per year over the next 5 years, media time online and on mobile devices is growing at increasing rates while TV, print and radio time is flat or declining, and sophisticate mobile devices have radically changed employee access to enterprise and government information. The onset of convergence of online and mobile applications and services without identity federation has resulted in significant security and identity management challenges across the online ecosystem – in short, online identity is broken due to the re-use of passwords across the Internet.

Attribute Exchange as defined herein is designed to increase the use of trusted attributes online with minimized friction. In short, users assert and grant permission to bind their verified real world and online identities to enable online transactions based on services that employ interoperable technology and legal standards to enable predictable and enforceable transactions at Internet scale.

In general, efficient online identity ecosystems are expected to drive markets faster and further. Simply stated, reliability plus repeatability yields trust. The use of verified attributes across the Identity Ecosystem increases trust and decreases transaction friction. Trust results in predictable behavior which drives quantitative and qualitative metrics and benefits (Figure 7).

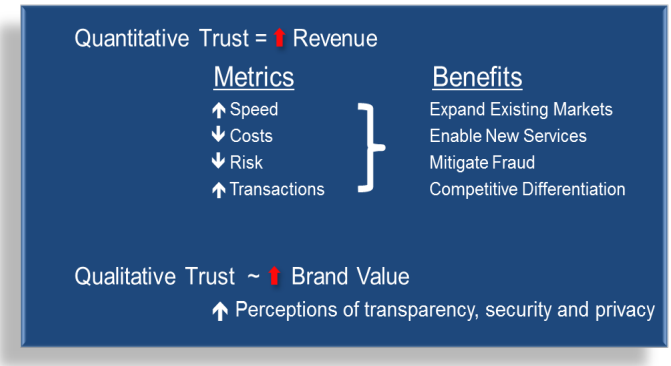


Figure 7: Attribute Exchange Market Motivators

Real world use cases often explore a basic set of business questions:

1. How do I connect a digital identity presented to my web site to a real person:
   - Simply? (interoperable APIs and policy management)
   - With minimal friction to my customer? (privacy protective, opt-in / opt-out)
   - At an affordable price point? (open, competitive attribute exchange market place)
   - Scalably? (web single sign-on)
   - With appropriate confidence? (minimal transaction risk)
2. How do I obtain real world information to support user transactions that:
   - Minimizes what I have to ask?
   - Allows me to market/communicate to them more effectively?
   - Increases the array of value-add services I can offer?

- Reduces my fraud loss rate?

Corporate IT and security departments have additional objectives including:

3. Cloud implementation of:
   - Real-time information verification services
   - Authoritative information sources
4. Reduce account creation and maintenance costs
   - Customers single sign-on to site using a login that they know and reduce drop off with full baskets
5. Additional signals including:
   - Strength of authentication credentials
   - "Step up" process verification and information for high risk or sensitive transactions
6. Select appropriate information/attribute sources based on:
   - Confidence level
   - Price point
   - Coverage
   - Tiered verification mechanisms to ensure widest geographic coverage
7. Select information sets to meet the needs of specific transaction types (FIPPS data minimization)

Benefit	AXN Value Proposition	AXN Benefits To Participants				
		AP	IDP	RP	User	Others*
Increase Revenue	**Improve user experience and trust, and increase transaction volumes**	✓	✓	✓	✓	✓
	Enhance target marketing and offer higher value services	✓	✓	✓	✓	✓
Reduce Costs	**Low cost, rapid implementation via Attribute Exchange Network (AXN)**	✓	✓	✓	✓	✓
	Real-time, affordable access to verified, user-permissioned attributes	✓	✓	✓	✓	
	Standards-based APIs for ease of technical interoperability	✓	✓	✓		✓
	Lower costs via the online "Network effect" while expanding addressable market	✓	✓	✓		✓
	Online market gateway for affordable, higher LOA identity services to reduce fraud	✓	✓	✓	✓	
Increase Trust	**Manage user privacy along with regulatory and organizational conflicts of interest**	✓	✓	✓	✓	✓

Figure 8: AXN Value Proposition

Each participant on the AXN is motivated by the prospect of increasing revenue, reducing costs and increasing trust with their customers, partners and stakeholder communities. The benefits of participation in the APN and Pilot Use Cases are shown in Figure 8. For APs, the AXN is an online market channel that efficiently manages attribute processing without incurring conflicts that can arise from AP, telecom, and financial services industry regulatory constraints, market channels, or how AP data has historically been aggregated without user permissions for monetization. By participating in the AXN, APs simply verify attributes that have been asserted by a user and do not provide or disseminate actual user attribute data to the AXN. As such, the AXN is an additional market channel for APs to access RPs online that simplifies their ability to efficiently participate, deploy new identity attribute services, and monetize existing attribute assets to the community of RPs.

Relying Party Market Development

It is estimated that APs currently only support between 15-25% of the total addressable market for attribute verification, leaving approximately 75% of the market without an implementation mechanism. These APs employ direct sales models that do not efficiently support small to medium-sized RPs, and regularly deny service to this market segment. The AXN enables three strategies to drive RP adoption:

- Partner with leading APs that typically employ direct sales strategies to large RPs. The AXN offers the benefits described above to these large APs and RPs.
- Implement OpenID Connect through the online Identity Ecosystem with leading IDPs using the AXN attribute exchange service across the Internet.
- Deploy the AXN attribute exchange service in conjunction with Business Cloud Networks to establish trust in the cloud for federated identity services for enterprises, including small and medium-sized business that currently are not addressed by large APs.

Relying Party participation is essential to supporting the AXN business model since they pay for the AXN services. In general, high level value propositions for RPs start with:

1. Federated Login
    - Simplify and increase sign-up/sign-in
    - Lower help desk costs
    - Improve security & reduce fraud
    - Strengthen trust and brand
2. Online Identity Attribute Exchange
    - Stronger authentication
        - User asserted, verified & permissioned attributes
        - User-centric privacy controls
        - "Step up" process verification and information used for contextual authentication for high risk or sensitive transactions
    - Reduce cost of identity attributes per user
    - Single stop shopping for attribute verification services via a competitive market space
    - Sell higher value products/services
    - Improve target advertising
3. Advanced Online Applications (e.g., APIs)

In the short term, RPs will be motivated to develop advanced APIs to differentiate their service offerings, increase user participation and reduce costs. Over time, the AXN implementation strategy is self-sustaining and is based on an AXN monetization business model for each participant in the ecosystem. This business model will evolve to align with policy and technology advancements to be self-sustaining, fully realized, and available to the user community. This will ensure all implementation actions are complete and all required policies, processes, tools, and technologies are proven and continue to evolve to support the Identity Ecosystem. RPs will choose to be part of the trusted Identity Ecosystem and implement trust frameworks to realize significant market efficiencies and reduced costs. Internet users will regularly engage in trusted online transactions because it is simpler, safer, and more private. These transactions will be verified through an Identity Ecosystem that sustains and expands a market for the trusted, efficient, and audited exchange of identity online attribute claims.

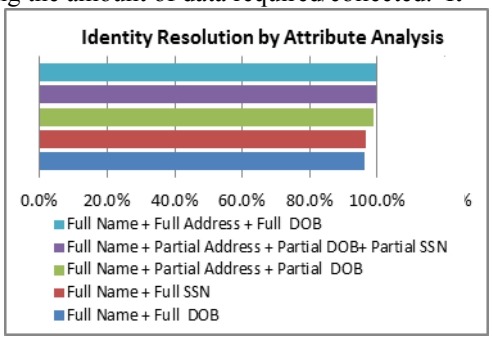
Data Model Definitions

A major goal has been to facilitate innovation in the attribute market by offering a broad array of attributes and providers, supporting a fusion between traditional approaches and emerging techniques and attribute types.

- Core Attributes
- Verification Checks
- Social Media Attribute Vetting
- Analytic Scores – Levels of Confidence
- Out-of-Band Authentication

Core identity attributes are used by RPs to assist in establishing uniqueness, resolving to a unique identity with increasing accuracy, and addressing privacy concerns around minimizing the amount of data required/collected. It turns out that a small number of core identity attributes are required for most RP use cases, and the AXN is ideally suited to update user attribute claims and data to support a wide array of RP use cases (Figure 9). Those core identity attributes include:

- Name (First, Last, Middle)
- Address (House #, Street Name, City, State, County, Postal Code)
- Date of Birth (Month, Day, Year)
- SSN4 or SSN9 (or other Government Identifier)
- Email Address
- Telephone Number (Country Code, Area Code, Prefix, Line #)



One primary goal is to create a marketplace to identify, compare and select attribute verification services more easily:

- Identify: Easy-to-use wizards to identify attributes and attribute providers
- Compare: "Nutrition labels" and data sheets to facilitate comparisons of available attributes (Figure 10).
- Select: The ability to select multiple attribute providers in one transaction to fulfill the need for the requested attributes.

Data model definitions and attribute metrics (Figure 11) have been defined to facilitate:

- Consistency in the manner that attributes are referenced
- Standardization across attribute providers
- Development of a monetization model

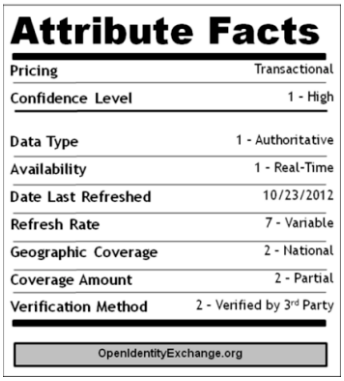


Figure 9: Attribute Facts

Data Type	Metric
Authoritative	5
Aggregated	4
Direct Captured	3
Self Asserted	2
Derived	1
N/A	0

Availability/ Timing	Metric
Real-time	1
Not Real-time	0

Geographic Coverage	Metric
Global	3
National	2
State/Provence	1
N/A	0

Refresh Rate	Metric
Real-Time	5
Daily	4
Weekly	3
Monthly	2
Annually	1
Never	0

Verification Method	Metric
Verified by Issuer	4
Verified by 3rd Party	3
Out of Band	2
Not Verified	1
N/A	0

This is a derived attribute

Level of Confidence	Metric
High	3
Med	2
Low	1
None	0

Coverage Amount	Metric
Full	3
Partial	2
Minimal	1
N/A	0

Currency/ Refresh Date
Actual Date

LOC (level of confidence) = fcn(Data Type, Verification Method, Refresh Rate, Currency)
Pricing = fcn (LOC, Coverage, Attribute Type)

Figure 10: Data Model and Attribute Metrics

- Attribute Definition: An inherent characteristic or metadata of an object
  Source: http://www.unece.org/fileadmin/DAM/stats/publications/53metadaterminology.pdf

- Data Definition: The physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means.
  Source: http://www.unece.org/fileadmin/DAM/stats/publications/53metadaterminology.pdf
- Data Element Definition: A smallest identifiable unit of data within a certain context for which the definition, identification, permissible values, and other information is specified by means of a set of attributes.
  Source: http://www.unece.org/fileadmin/DAM/stats/publications/53metadaterminology.pdf

Data Types

An AXN relies on AP services to verify user attribute data, and each AP service is comprised of one or more sources of data that can be categorized by one or more of the following data types:

Authoritative: Data created by an originating source and/or exclusively controlled by a source responsible for a particular set of attributes associated to those instances. For data to be authoritative there must exist a single point of provenance with exclusive jurisdiction over all or a known subset of values within the domain. An essential element of an authoritative attribute is that it is associated to an instance of an index which is unique within the jurisdiction.

Short Definition: Data originating either from the original author or creator of the data, or from a licensed reseller of that source or sources.

Example: A social security number and name from the social security administration. A telephone number, name and address from a phone company; an address from the Post Office; a date-of-birth or date of death from a government department of vital records.

Aggregated: An attribute or attribute set assembled from values independent of a common, exclusively controlled provenance and which contains the majority of the content of the original independent values. A notable difference between this and a derived value is that instances of derived values are generally not within the same domain as the independent values from which they were derived. Aggregation implies some merging of distinct and independent data flows.

Short Definition: A data set created by combining individual elements of data from multiple sources, some of which may be authoritative.

Example: A common example of aggregated data is combining the name associated to a street address and the phone associated to that same street address into a single aggregate result of name, street address and phone. The end result is largely the same as the original input values.

Direct Captured: An attribute whose value was obtained neither from an authoritative source, nor was functionally derived, nor from the data subject over which the subject has control itself unless the attribute was derived from a distinct physical characteristic.

Short Definition: Physical collection of data contained in an object about a subject.

Example: A credit card number obtained by examination of a physical card provided by an authoritative entity (who is responsible for all attributes associate to that unique card number) to an identity subject for their use as a trusted token. An iris scan or fingerprint would also qualify as direct capture.

Self-Asserted: An attribute value that was provided by the subject about which the attribute is referring.

Short Definition: Any information asserted by a subject.

Example: A date of birth requested as part of a social network account profile registration process.

Derived: An attribute obtained by applying a mathematical or logical process to one or more attributes. The nature of a derived attribute is that it is functional in the mathematical sense so that one and only one value exists for the same set of inputs. Derivation implies a transformation from one set of values to another.

Short Definition: A value calculated by a proprietary rule set.

Example: A credit score.

Additional definitions for the data model and attribute metrics can be found in the table below:

Metric		Definition
Availability	Real-time	Average response returned within 5 seconds
	Not Real-time	Average response returned in greater than 5 seconds
Geographic Coverage	Global	Data coverage across multiple countries. Country list describes specific location coverage and respective coverage amounts.
	National	Data coverage within a country, representing multiple states or provences. State/Provence list describes specific location coverage and respective coverage amounts.
	State/Provence	Data coverage within a state or provence. State/Provence list describes specific location coverage and respective coverage amounts.
	N/A	No geographic coverage/ Not applicable
Coverage Amount	Full	Data coverage represents 90+% of the geographic area, domain or service
	Partial	Data coverage represents 40-90% of the geographic area or service
	Minimal	Data coverage represents less than 40% of the geographic area or service
	N/A	No data coverage
Verification Method	Verified by Issuer	Verification performed by issuer of the attribute
	Verified by 3rd Party	Verification performed by a third party attribute provider
	Out of Band	Verification performed by confirming one time passcode sent to phone via SMS text or audible telephony or to an email address
	Not Verified	No verification of the attribute has been performed
	N/A	Not applicable
Refresh Rate	Real-Time	Data is refreshed/updated as soon as changes occur or within 12 hours
	Daily	Data is refreshed/updated at least once per day
	Weekly	Data is refreshed/updated at least once per week
	Monthly	Data is refreshed/updated at least once per month
	Annually	Data is refreshed/updated at least once per year
	Never	Data is never refreshed

Figure 11: Data Model Definitions and Attribute Metrics

Compliance Requirements and Regulations

For each prospective RP to whom the AXN proposes to provide information must be investigated by AXN operations staff prior to the RP having access to information provided by APs who offer data from regulated data sources. As such, the AXN staff must:

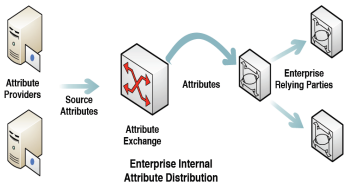
- Confirm that the RP is a legitimate business entity and in good standing in the state(s) and country(ies) in which it does business and has all required licenses;
- Confirm the RP's business type;
- Confirm the RP's business location and location type (for example, residential or commercial office space);
- Confirm and receive appropriate certification that the RP will/will not be accessing information for purposes allowed by the Federal Fair Credit Reporting Act ("FCRA") (whichever is applicable) and in accordance with AP policy;
- Confirm that the RP has an appropriate permissible purpose for accessing such information governed by the Gramm-Leach-Bliley Act ("GLBA") and/or Driver's Privacy Protection Act ("DPPA") and will only access such information for such permissible purpose, where applicable;
- Confirm that the RP has appropriate data and access security procedures and programs, in compliance with applicable industry standards and AP policy; and
- Develop and implement a defined audit program designed to monitor the usage of its RPs to reasonably prevent and detect unauthorized use of AP, AXN and IDP systems or information.

The AXN must complete all above requirements ***prior*** to allowing information access by the RP. If any of the above requirements are not met, the AXN shall not provide AP information to the RP.

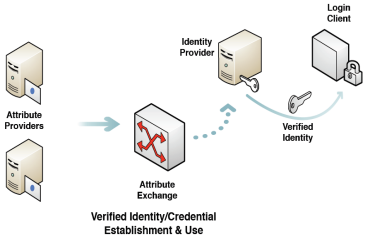
AXN Monetization Model

An Attribute Exchange can support a number of different monetization models for verifying user-asserted attributes and delivering trusted online attribute verification services. In general, revenues for the AXN service are paid for by participating RPs at open market prices established by APs via service contracts on a per transaction or annual subscription model basis. RP pricing for attribute verification services through the AXN as an annual subscription is estimated to range in price depending upon the data type (e.g., authoritative self-asserted, derived, direct from source), market coverage, data quality/freshness and the Level of Confidence (LOC) associated with the verified user attributes. Listed below are those most commonly encountered models; however, it is not intended to be an exhaustive list. Direct to RP is a case where the AXN is not directly involved in the transfer of attributes but may have been engaged in setting up some a priori arrangement at a contractual level. This may or may not involve the user in the transaction flow, and is not presented as a use case.

The Simple Attribute Exchange model is what most of us think about when we think attribute exchange, and has various implications about payment for each request, refresh of information, and possibly some processing at the AXN. The Simple Attribute Exchange is typically priced per transaction, but RPs with a high frequency of user logins have expressed strong interest in per user per year pricing. RPs will want to specify the frequency of attribute refresh in their negotiated service contracts since RPs will generally pay each time a user's attributes are refreshed.



The Enterprise Internal Distribution model builds upon the Simple Attribute Exchange. The enterprise is comprised of several relying parties all using the procured attributes. In many cases, the AXN will verify user attributes via commercial AP services. In addition, some of the enterprise attribute sources could be considered authoritative in the case of employment related attributes including employee status, role, employee number, etc. This model may require defining the boundaries for acceptable reuse and limitations regarding the size of the enterprise, for example, the multiple agencies within a National Government.

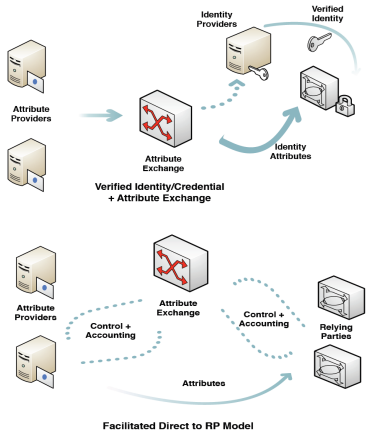


The Verified Identities model is a very specific case where an IDP may use attributes from APs to run through a verification process for identity proofing which establishes an identity and credential at some assurance level. The credential and identity may only be used for sign-on authentication activities

and no further attribute may be requested or required by the relying party that is primarily a login client. The issue of what or how much revenue could be accrued back to APs if the IDP sells it service to additional RPs is undetermined. In general, the IDP is creating value based on its verification processes and that the raw attributes used in that process are not conveyed to the RP.

Similarly, the Verified IDs with Attributes uses an IDP for a verified identity but also wants to access some associated attributes – in the image below, it is shown as two "interactions" but could be implemented in many ways.

The final model, Facilitated Direct to RP model, is where an AP and an RP directly interact in the sharing or attributes, but control of access, billing and auditing are functions provided by the AXN.



Trust Elevation

The level of assurance needed for a specific RP service is based on the consequence of authentication errors and/or misuse of credentials. As the consequences of an authentication error increase, the level of assurance (LOA) should increase. Informal or low value requirements will require less stringent assurance while higher value or legally significant services (e.g., medical) will require more stringent assurance. In general, RP security teams map identified risks for a particular RP service to an appropriate credential authentication level based on potential impact. In most cases, assignment of impact to these risks is based on the context and nature of the people or entities affected by an improper authentication.

RP privacy policy often influences the minimum data required to verify the identity of an individual. An AXN can support a broad array of methods for minimizing the data that is ultimately needed to be shared with RPs for their purposes of authenticating a user while still supporting RP risk mitigation requirements. This dynamic, along with the evolution of efficient online identity technologies, enables a portfolio of options for measuring value and trust elevation associated with credentials and verified attribute claims as shown in Figure 13 below.

Verified Attribute Claim	AXN Trustmark Services			
	TM1	TM2	TM3	TM4
Pii	Name+ Email+ Address + Telephone (NEAT)	TM1 + DOB	TM2 + SSN4	TM3 + SSN9
Device	Pii + SMS PIN + IPSEC	TM1 + Device ID	TM2 + MDM	TM3 + GEO
Biometric	None	Pii + Device + Voice (Bio1)	TM2 + Bio2	TM3 + Bio3
PKI Credential	None	None	Pii + Device + PKI	TM3 + Biometric

Low
$ Cost
Higher
Low
$ Cost
Higher

Figure 12: AXN Trust Evaluation Services for LOA with Verified Attribute Claims

An AXN Trustmark is a set of practices from service providers that will elevate online transaction trust where individuals can conduct sensitive business transactions online with reduced fear of identity theft or fraud and without the need to manage scores of usernames and passwords. It leverages commonly used technology components such as cell phones, smart cards, and personal computers to act as or to contain a credential. These

identity solutions are built into online services to enhance their usability and user trust. It offers a suite of multi-factor authentication methods to securely access sensitive data and applications using a persistent identity credential for federated internet single sign-on.

Starting with a federated single sign-on credential (e.g., SAML, OpenID), an AXN can be used to bind verified user attributes, SMS text or voice message with a PIN code, device identifiers, and biometric attributes to generate attribute and authentication claims to support complex requirements for higher levels of assurance. By leveraging the user's existing phone, mobile device PC or laptop, an AXN can enable trusted services and convenience for users and a cost-effective, secure platform for RPs. Users require no training and no ongoing support, making an AXN inexpensive to configure and maintain. No additional tokens are purchased, provisioned, managed, and renewed, so AXN services can enable rapid, cost effective deployment with existing user devices online anywhere and anytime.

Trust Framework Enrollment Strategy

In general, a given trust framework will grow and succeed based on the adoption of the online services marketed to users for which they agree to have their identity verified in compliance with required processes and procedures. An early objective will be to identify the RP services available or contemplated that require higher levels of assurance that will drive growth, define the risk mitigation requirements, and to develop an implementation plan to drive User adoption. More specifically, this effort must establish a pragmatic go-to-market strategy and the implementation process for driving RP participation as both consumers and providers of trust framework services.

As a new trust framework community of interest emerges, a group of organizations will present an opportunity to gather participation and to build momentum in the new trust framework. A plan must be developed to engage quietly at first to better understand the strategy and needs of this group. When it appears as if some participants in this group might become great lead RPs, the plan must identify resources (human and capital) required to provide the group with the vision of how to bridge to online/federated trust framework operations. The key is for the trust framework model to become the enabling force that the group can leverage to build/expand business in the online space.

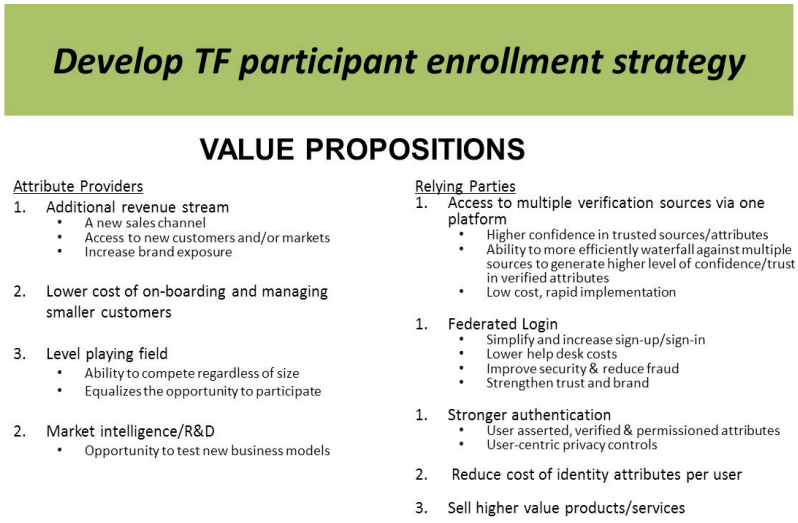


Figure 12: TF Participant Enrollment Strategy

For any new trust framework, an action plan will be required to engage with industry RPs to educate about the opportunities/benefits and evangelize to create and drive momentum. Having the OIX Board and existing community member influence is essential and will help build credibility. Each trust market participant will likely have different wants/needs/concerns, so it will be essential to find one or two lead participants and to spend resources to generate market momentum based on competitive pressures.

AXN Legal Framework

Introduction

In any situation where multiple parties come together to achieve common goals, whether in social communities, commercial markets or political governance structures, sets of interdependent rules, specifications, and agreements are often at the core of the arrangements. Such documents set forth the respective duties, rights and expectations of the parties, and provide common features such as change processes, enforcement mechanisms and the like. The AXWG Legal portion of an Attribute Exchange Trust Framework Specification for a COI should address the structural and content issues necessary to develop an enforceable set of such interdependent rules, specifications, and agreements.

An Attribute Exchange Trust Framework consists of a combination of business model processes and procedures, technical standards and systems, contractual agreements with legal rules, privacy policies, certification standards and audit procedures that, taken together, establish a trustworthy system for: (i) verifying and assigning identity attributes and connecting those identity attributes to an individual human, legal entity, device, or digital object, (ii) providing that identity attribute information to a party that requires it to complete a transaction, and (iii) maintaining and protecting the identity attribute information over its lifecycle. Critical to making it work for a community of interest in a business, government and commercial context is the requirement for an appropriate, and typically voluntary (e.g., contractual) legal framework (sometimes referred to as "operating rules" or a "trust framework") that defines the rights and responsibilities of the parties, allocates risk, and provides a basis for enforcement. The objective is to implement a capability for the secure, reliable and trustworthy exchange of digital identity attribute information that can be used remotely across different systems and entities.

Participants of the OIX AXWG Legal Group

- Edwards Wildman Palmer LLP - Tom Smedinghoff
- LexisNexis – Federico Bucspun
- LexisNexis – Katie Ray
- ID DataWeb – John Dials
- ID DataWeb - Dave Coxe
- Domenic Dillulo – Accenture (formerly Department of Homeland Security)
- Naomi Lefkovitz – NIST, NSTIC Senior Privacy Advisor
- Dale Rickards - Verizon

Identity Management System Risks

As a first step in developing legal contracts, it is important to understand the overall risks that they need to address. There are several potential risks to participating in an attribute exchange network and using and relying on identity and attribute data exchanged via that network. These risks were initially identified by the American Bar Association Identity Management Legal Task Force[1] as some of the key risks that must be addressed before participants will have trust and confidence in the operation of an identity system, and apply equally to an attribute exchange network.

While these risks affect all participants in an attribute exchange, the way in which the risks affect each participant and the significance of the risks to each participant will, of course, vary by the role such participant is fulfilling at any particular point in time. The risks may be summarized as follows:[2]

- **Identification Risk:** The reliability of the identity information collected, verified, and asserted about the User is critical to the use of any identity system. Identification risk is the risk that identity attribute data collected and associated with a specific User (e.g., an individual, entity, or device) is inaccurate. This risk is often a function of the quality of off-line identity credentials provided by the User for identity verification.

[1] See http://apps.americanbar.org/dch/committee.cfm?com=CL320041

[2] See ABA IdM Report – Part 1 – 12/30/2011 Draft, available at http://apps.americanbar.org/dch/committee.cfm?com=CL320041.

- **Authentication Risk:** Identification is of no value unless a Relying Party that seeks to rely on such identification has the ability to reliably authenticate it – i.e., associate the claimed and verified identity attributes to the correct User. Authentication risk includes both the risk that a legitimate User cannot be properly authenticated, as well as the risk that an authentication process will incorrectly indicate that an imposter is a legitimate User.
- **Privacy Risk:** In the case of individuals, identity management involves the collection and verification of personal information about a User by an Identity provider via the AXN and the sharing of that information with multiple Relying Parties. In addition, identity-based transactions may also facilitate tracking an individual's activities, thereby generating additional personal information. Privacy risk focuses on the unauthorized use or misuse of personal information about the User by one of the parties who has access to it, as well as on their compliance obligations with respect to the processing and protection of such data.
- **Data Security Risk:** Protecting personal information about human Users, as well as maintaining the security of the processes necessary to create secure identity credentials, verify and communicate accurate identity information, verify the status of identity attributes and credentials, and authenticate Users, is critical to any identity system. Security risk includes both the risk that an unauthorized party can obtain access to personal data, as well as the risk of compromise of one or more of the processes critical to the overall functioning of the identity system or any individual identity transactions.
- **Liability Risk:** In any identity system, failures will inevitably occur, and damages will result. Participants in an identity system must address the risk that they will be held liable for damages suffered by someone else resulting from a problem they caused or for which they are deemed legally responsible. A key aspect of the liability risk is the legal uncertainty regarding the responsibility that attaches to any given act or failure to act by a participant in an identity system, particularly one that operates across multiple industry sectors and jurisdictions.
- **Enforceability Risk:** Enforceability risk is complimentary to liability risk. It is the risk that one participant will not be able to enforce (i) its right to compliance with the rules by another participant, or (ii) its right to collect damages in event it is actually harmed in a case where another participant is legally "liable." This risk applies when something goes wrong and someone seeks to recover damages. It also applies in situations where a problem has not yet surfaced, but a failure of performance on the part of one or more participants can put the entire identity system at risk. This is particularly important in a cross-jurisdictional system. In such case, enforceability risk refers both to the ability to detect that problem, as well as the ability to require the participant to remedy its performance or withdraw from the system.
- **Regulatory Compliance Risk:** In many cases, participation in an identity system raises legal compliance issues for one or more of the participants – i.e., whether the conduct of the participant complies with applicable local law. In other cases, participation in the identity system is, in and of itself, pursued in an effort to comply with legal requirements imposed on a participant. For example, a financial institution may participate, and rely on identity credentials and verified attribute claims to satisfy its legal obligations to properly authenticate individuals granted online access to bank accounts and payment facilities. In such cases, compliance risk focuses on whether such participation satisfies it legal obligations.

As with any system or process, the foregoing risks are a function of the technology used, the various processes implemented, and the manner (or failure) of performance of obligations by the participants (in addition to possible influence by outsiders). Building a reliable AX Trust Framework will require measures to address these risks – that is, measures designed to ensure that participants can trust the technology used (i.e., that it works properly), the processes deployed (i.e., that they yield the correct result), and the other participants (i.e., that they will properly perform their obligations).

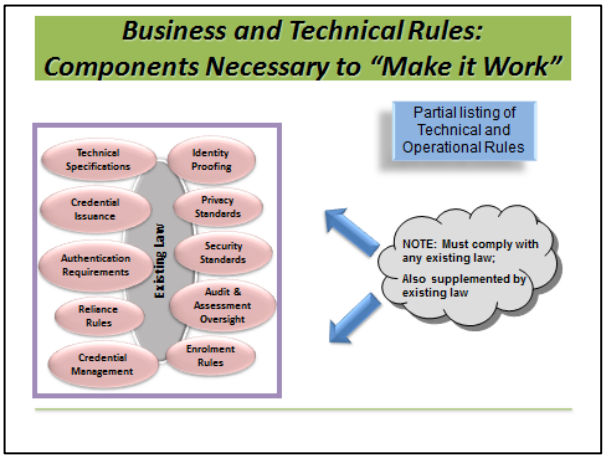
Addressing Functionality and Risk -- Trust Framework Operating Rules

Every multi-party transactional system, where participants will interact with multiple parties, such as an identity system, a credit card system, or an electronic payment system, has three basic requirements. An attribute exchange network is no exception. Those requirements are:

- A common set of rules must exist (to make it work, and to address the applicable risks);
- Each participant must agree to follow those rules applicable to it, for the benefit of the other participants affected by its performance; and
- Each participant needs some reasonable level of assurance that all of the other participants will follow the rules.

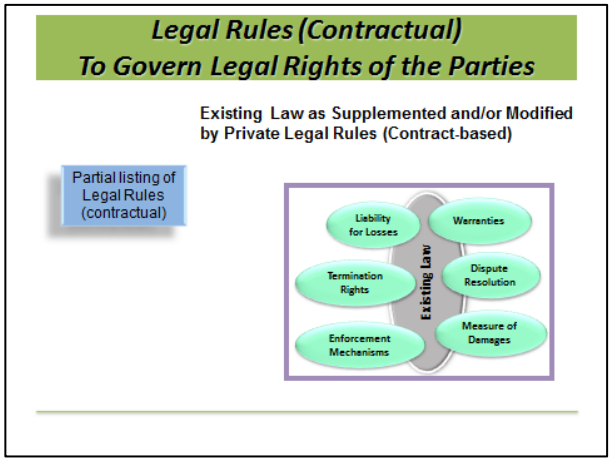
Thus, making an AXN work in an online environment, and addressing the risks such as those noted above, requires not only the implementation of appropriate technology, but also adherence by all participants (e.g., Subjects, Identity Providers, Attribute Providers, and Relying Parties) to a common set of technical standards, operational requirements, and legal rules. Commercial identity systems typically seek to achieve that goal by developing an appropriate "Trust Framework" (sometimes referred to as "operating rules") to which participants are contractually bound.

Such a Trust Framework consists of two general categories of components: (i) the business, privacy, and technical operational rules and specifications necessary to make the system functional and trustworthy, and (ii) the contract-based legal rules that, in addition to applicable laws and regulations, define the rights and legal obligations of the parties specific to the identity system and facilitate enforcement where necessary.[3]



The business and technical operational rules (Figure 15) define the requirements for the proper operation of the identity system (i.e., so that it works), define the roles and operational responsibilities of the participants, and provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data (i.e., so that the various parties are willing to participate; so it is trustworthy). In many cases, such rules are built on existing standards.

The contractual legal rules (Figure 16) consist of the contract-based agreements between or among the participants that define and govern the legal rights, responsibilities, and liabilities of the participants with respect to the specific identity system, clarify the legal risks parties assume by participating in the identity system (e.g., warranties, liability for losses, risks to their personal data); and provide remedies in the event of disputes among the parties, including methods of dispute resolution, enforcement mechanisms, termination rights, and measures of damages, penalties and other forms of liability.



They also make the business and technical operational rules legally binding on and enforceable against the participants. Both the business and technical rules and the contractually-defined legal rules are, of course, subject to, and typically constructed with reference to, other existing duties and obligations arising under the statutory and regulatory law that apply to the parties. Taken together, these business and technical operational rules and contractually-defined legal rules comprise the identity system operating rules (or trust framework).

It goes without saying that laws relating to data protection, privacy and use of personal information must be obeyed where they apply. All contractual arrangements must be compliant with regulations pertaining to personal data sharing, protection and retention. The remainder of this outline will focus on the risk allocations and contractual terms that should be addressed regardless of the applicable laws.

Law Governing Attribute Exchange Networks

In most jurisdictions there are numerous existing laws and regulations that will have a significant regulatory impact (and which may impose barriers, compliance requirements, and/or liability risk) on participation in an attribute

[3] See ABA IdM Report – Part 1 – 12/30/2011 Draft, available at http://apps.americanbar.org/dch/committee.cfm?com=CL320041

exchange network. In addition, differences among the laws of different jurisdictions, when considered in light of the global nature of the internet, create a patchwork regulatory landscape that can itself challenge legal structuring.

Some of these laws and regulations focus specifically on identity-related activities. Most, however, were developed in a context completely unrelated to identity management (e.g., tort law, contract law, and warranty law), but may nonetheless have a significant impact, and often in ways that were unanticipated at the time of their original adoption.

Developing contract-based operating rules for an attribute exchange network is the primary method of addressing the legal challenges associated with efficient, interoperable, and acceptable systems that can operate cross-border and reduce uncertainty for participants. It also facilitates experimentation with different systems and different approaches as the marketplace works to develop solutions to the issue of attribute exchange. All participants in an attribute exchange network have an interest in fairly allocating, in advance, the risk of liability that flows from participation in the process, as well as mitigating those risks to the extent possible. As attribute exchange network processes are used for increasingly significant transactions, and the risks to the parties increase accordingly, the benefits to all parties of implementing appropriate operating rules to address those risks up front, as well as to mitigate those risks (to the extent possible) by requiring performance of specific obligations by each participant role, is significant.

Attribute Exchange Trust Framework Legal Requirements

The AXWG Trust Framework specification contemplates a set of system operating rules (Figure 17) made enforceable on the participants by a set of legally binding agreements (Figure 18).

1. Operating Rules

The ultimate goal of any attribute exchange network is to provide identity and attribute assertions that are sufficiently reliable for the intended purpose, and to do so in a manner such that all relevant parties are willing to trust it – i.e., to participate and rely on the results. Achieving that goal requires developing and implementing a set of legally binding operating rules to govern the activities of the participants in, and the operation of, the attribute exchange, and to do so in a manner that addresses the risks identified above.

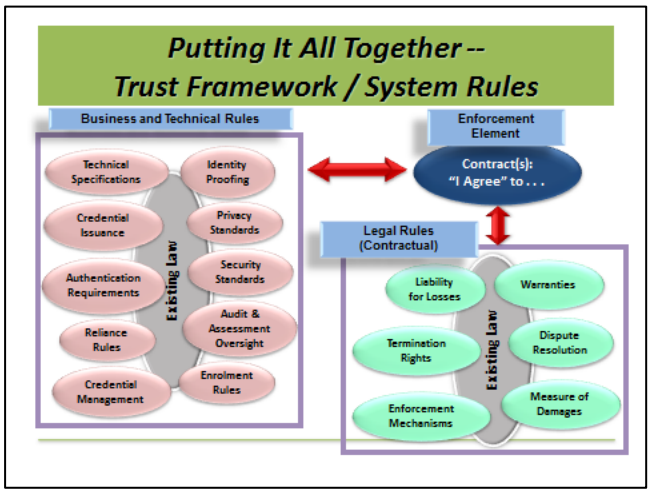


Figure 15: Trust Framework / System Operating Rules

The use of such operating rules is typically necessary to govern the functioning of multi-party systems used to accomplish a specific functionality. Generally, such operating rules should accomplish the following:

- First, the operating rules should address the key system-specific business, technical, operational, privacy, and legal issues necessary for the attribute exchange to function properly and achieve the desired result – i.e., so that it works. This might include, for example, rules regarding the procedures that must be followed by each participant, the format for exchanges of identity attribute data, the way in which software must handle identity attribute data, and the processes and procedures each participant will be expected to follow to make it all work. Such rules will also typically define the rights and responsibilities of all participants, security requirements, transmission standards and formats, response time standards, liabilities, exception processing, error resolution and the like. Beyond making the identity system work, and reducing cost and administrative hassles, such rules also foster trust among all participants in the identity system.

- Second, operating rules should be designed to address the seven risk categories noted above. By requiring the use of certain technology and business processes, and by imposing certain obligations on the participants, the

rules can be designed to mitigate the risks of greatest concern to the participants. This also helps to foster trust among all participants in the identity system – i.e., a willingness to participate and to rely on the results.

Familiar examples of such operating rules include the various rules that govern the processing of payment transactions. For credit card transactions, credit card system rules (such as the Visa Operating Regulations) provide the specifications and rules applicable to the participants in a credit transaction and subsequent processing.

In many cases an entity often referred to as a Trust Framework Provider (TFP) is established to develop and implement the operating rules for the Trust Framework. That is, the TFP is responsible for establishing the business, legal, technical, privacy, certification and audit policies for the Trust Framework.

The operating rules for the Trust Framework become the contract(s) and policy document(s) that specifies the requirements to which the trust framework members must adhere.

2. Operating Agreements

The operating rules for an attribute exchange Trust Framework are of little value unless the various participants in the attribute exchange actually agree to follow the rules. This is typically done by contract (e.g., as in a credit card system).

Many different forms of agreement can be used. And the agreements can directly incorporate all of the operating rules, or simply incorporate them by referencing the master document. In either case, however, it is anticipated that the following agreements (among others) will likely be required (Figure 18):

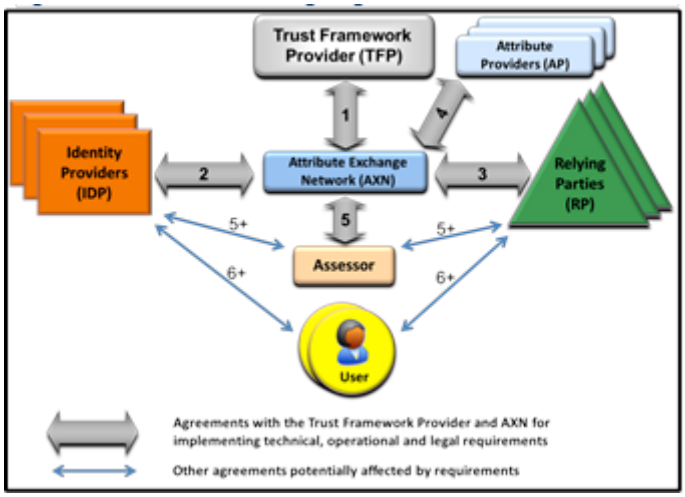


Figure 15: Trust Framework Legal Agreements between Parties

1. **Trust Framework Provider Service Agreement –** Defines legal, technical, and operational requirements for a Community of Interest established by policymakers embodied in the TFP organization for a specific set of industry and business requirements. Such contract binds the AXN to the applicable terms of the operating rules, and obligates the AXN to incorporate such terms in its contracts with the other roles.
2. **Identity Service Provider Agreements –** Contracts between the AXN and IDPs who have been certified by an assessor as meeting the technical, operational, and legal requirements of the trust framework. Such contracts bind the IDPs to the applicable terms of the operating rules.
3. **Relying Party Agreements –** Contracts between the AXN and RPs who have been certified by an assessor as meeting the technical, operational, and legal requirements of the trust framework. Such contracts bind the RPs to the applicable terms of the operating rules.
4. **Attribute Provider Agreements –** Contracts between the AXN and certified APs who have been certified by an assessor as meeting the technical, operational, and legal requirements of the trust framework. Such contracts bind the APs to the applicable terms of the operating rules.
5. **Assessor/Auditor/Certifier Agreements –** Contracts between the TFP or AXN and individual entities acting as an assessor authorizing such assessor to evaluate prospective participants in the AXN to determine whether such entities meet the applicable requirements of the operating rules for the trust framework. These agreements bind Assessors to use a standard set of TFP-recognized and enumerated processes when they conduct assessments.
6. **Terms of Service (TOS) Agreements –** Designed to establish rights and responsibilities for users that do not already have TOS agreements with IDPs and RPs. The TFP promotes a set of model terms that are included by IDPs and RPs in their TOS agreements with users

AX Trust Framework Legal Checklist

In developing the trust framework operating rules, certification requirements, and the associated contracts with the various participants, there are a variety of topics that will need to be addressed. Some of the more common topics that must be addressed are listed below, along with a listing of the contractual relationships where each should (or could) be addressed.

1. **Define Attribute Exchange Network (AXN) Roles**
   - **(a) Trust Framework Provider Role (TFP)**
     - (1) Specify the eligibility requirements for the role.
     - (2) Specify rights, duties, and obligations of participant filling such role
   - **(b) Attribute Exchange Network Role (AXN)**
     - (1) Specify the eligibility requirements for the role.
     - (2) Specify rights, duties, and obligations of participant filling such role
   - **(c) Assessor / Auditor / Certifier (Assessor) Roles**
     - (1) Specify the eligibility requirements for the role.
     - (2) Specify who approves an applicant to participate as an assessor in the Attribute Exchange Network.
     - (3) Specify rights, duties, and obligations of participant filling such role
     - (4) See generally "**AXN Assessor/Certification Framework**" within this document)
   - **(d) Identity Provider Role (IDP)**
     - (1) Specify the eligibility requirements for the role.
     - (2) Specify who approves an applicant to participate as an IDP in the Attribute Exchange Network.
     - (3) Specify rights, duties, and obligations of participant filling such role
   - **(e) Attribute Provider Role (AP)**
     - (1) Specify the eligibility requirements for the role.
     - (2) Specify who approves an applicant to participate as an AP in the Attribute Exchange Network.
     - (3) Specify rights, duties, and obligations of participant filling such role
   - **(f) Relying Party Role (RP)**
     - (1) Specify the eligibility requirements for the role.
     - (2) Specify who approves an applicant to participate as an RP in the Attribute Exchange Network.
     - (3) Specify rights, duties, and obligations of participant filling such role
   - **(g) End User Role (User)**
     - (1) Specify the eligibility requirements for the role, if any.
     - (2) Specify who approves an applicant to participate as an user in the Attribute Exchange Network, if necessary.
     - (3) Specify rights, duties, and obligations of participant filling such role
     - (4) End User Notice & Consent Obligations

2. **Assessment, Certification, and Trustmarks**
   - (a) Specify assessment and certification requirements
   - (b) Specify Trustmark requirements
   - (c) Specify Trustmark warranties, representations, and limitations
   - (d) See generally "**AXN Assessor/Certification Framework**" within this document

3. **Identity Credentials**
   - (a) Specify acceptable credential formats to be used as data source for attribute requests
   - (b) Specify eligible credential issuers
   - (c) Specify eligible Subjects / Users (for each credential type)
   - (d) Specify purpose, authorized uses, and limitations on credential use (for each credential type)

4. **Attribute Data**
   - (a) Specify attribute data format requirements
   - (b) Specify other attribute data requirements
   - (c) Specify attribute data verification and processing requirements

5. **Personal Data Access**

(a) Allocate responsibility for operation and maintenance of personal data access
(b) Specify contents of personal data storage
(c) Specify who has access and conditions of access(e.g.,user only)
(d) Specify data security for data access and storage
(e) Specify privacy policies for access and retrieval

6. Identification of Users

(a) Purpose

(1) Identify User sufficient for Attribute Provider(s) to locate requested attributes

(b) Core Identity Data

(1) What core identity data is required by the Attribute Exchange Network to obtain requested attributes?

7. Designation of Attribute Provider

(a) Specify who will select the Attribute Providers per use case (either the RP or AXN)
(b) Specify selection criteria per use case

8. Attribute Data Delivery

(a) Specify the attribute data delivery means to the Relying Party
(b) Specify the frequency and means of updating personal data and the attribute claim data
(c) Security
  (1) Specify the security measures required and responsible party (such as the AXN) for the delivery process
(d) Consider transaction completion time as an AXN performance requirement.
(e) Errors in attributes
  (1) User rights to know source of AP data
  (2) User rights to see/correct bad data
  (3) Issues RE: non-FCRA data
  (4) User rights in case of bad AP data

9. AXN Services

(a) Specify the AXN's obligation to verify information regarding
  (1) The Attribute Providers it offers
  (2) The IDPs it offers
(b) Specify the extent, if any, the AXN is responsible for
  (1) The quality/ accuracy of the attribute information it delivers
  (2) The security of the attribute data
  (3) The timing of its responses to RP requests
  (4) The availability (up-time) of the network
(c) Warranty Service (if any)

10. RP and AXN Reliance Requirements

(a) Obligations before reliance considered reasonable
  (1) Attribute within validity period
  (2) Status of credential checked
  (3) Transaction verified
(b) What are the procedures that must be followed as a pre-condition to reliance?

11. Fees For Services

(a) Specify which activities are subject to fees
(b) Specify who pays and who collects fees
(c) Specify price and model, e.g., per transaction or per time period
(d) AXN Use License, if required
(e) See generally "**AXN Business Framework – AXN Monetization Model** within this document

12. **Warranty And Liability Obligations**
    - **(a) Specify the representations, warranties and warranty disclaimers made by each role**
      - (1) Identity Provider (IDP)
      - (2) Relying Party (RP)
        - (A) E.g., warranty RE: User consent to access attribute data
        - (B) E.g., warranty RE: Intended use of attribute data, privacy, etc.
        - (C) E.g., warranty RE: Compliance with applicable privacy law
      - (3) Attribute Provider (AP)
        - (A) E.g., warranty RE: Source and/or nature of attribute data, currency, and reliability
        - (B) E.g., warranty RE: Compliance with applicable privacy law
      - (4) Attribute Exchange Network (AXN)
        - (A) E.g., warranty RE: Delivery of attribute data, privacy, etc.
        - (B) E.g., warranty RE: Compliance with applicable privacy law
      - (5) Subject / User
      - (6) Assessor/Certifier/Issuer of Trustmark
    - **(b) Specify the limitations on liability for each role**
      - (1) Identity Provider (IDP)
      - (2) Relying Party (RP)
      - (3) Attribute Provider (AP)
      - (4) Attribute Exchange Network (AXN)
      - (5) Subject / User
      - (6) Assessor/Certifier/Issuer of a Trustmark

13. **Indemnification Obligations**
    - (a) Specify the indemnification obligations for each of the following roles
      - (1) Identity Provider (IDP)
      - (2) Relying Party (RP)
      - (3) Attribute Provider (AP)
      - (4) Attribute Exchange Network (AXN)
      - (5) Subject / User
      - (6) Assessor/Certifier/Issuer of a Trustmark

14. **Intellectual Property Rights**
    - **(a) Specify Elements of the AXN Protected by Intellectual Property Rights**
    - **(b) Trademarks and logos**
      - (1) Who owns trademark rights (if any)
      - (2) Specify rights to use / license to use these trademarks
    - **(c) Copyright rights**
      - (1) Who owns copyright rights (if any)
      - (2) Specify rights to use / license to use these copyrights
    - **(d) Patent rights**
      - (1) Who owns patent rights (if any)
      - (2) Specify rights to use / license to use these patents
    - **(e) Trade secret rights**
      - (1) Who owns trade secret rights (if any)
      - (2) Specify rights to use / license to use these trade secrets

15. **Data Ownership / License Rights / Legal Restrictions on Use**
    - (a) Specify scope and terms of data rights and restrictions imposed on each role
    - (b) Specify legal restrictions on use of data
    - (c) See generally "**AXN Business Framework – Compliance Requirements and Regulations** at within this document

16. **Confidentiality Obligations RE: Attribute Data**
    - (a) Types of attribute data to be kept confidential

(b) Types of information considered non-confidential
(c) Release of confidential information
    (1) To law enforcement officials
    (2) As part of civil discovery
    (3) Upon owner's request
    (4) Attribute Exchange Network Provider other reasons or in other circumstances

17. Privacy Obligations RE: Attribute Data
(a) Personally Identifiable attribute data collected during process
(b) Personally Identifiable Data storage and access
(c) Privacy policy regarding use of data
    (1) AXN purposes related to the Attribute Exchange Network
    (2) Attribute Exchange Network other purposes
    (3) Relying Party purposes
(d) Notice to User
(e) Access by User to attribute data about him/her
(f) Security of attribute data
(g) Consent of User to the attribute verification process
(h) See generally "**AXN Privacy Policy Framework**" within this document

18. Security Obligations RE:
(a) The physical site where AXN Services are performed (including back-up sites)
(b) The procedures and processes used to perform AXN services
(c) The people involved in performing AXN services
(d) The hardware used to perform AXN services
(e) The software used to perform AXN services
(f) The networks used to perform AXN services
(g) The databases used in performing AXN services
(h) The communications methods used to perform AXN services
(i) The keys used to perform AXN services
(j) The records stored regarding the perform AXN services
(k) Data integrity and reliability requirements
(l) See generally "**AXN Technology Framework – Security Considerations**" within this document

19. Data Retention / Records Archival
(a) Specify the types of log file events should be recorded and archived
(b) Specify the retention period for the AXN records archival

20. Data Destruction Requirements

21. Disaster Recovery Obligations

22. Compliance Audits / Performance Audits
(a) Specify who should be audited
(b) Specify who has right to conduct audit
(c) Specify the purpose and scope of audits
(d) Frequency of compliance audit for each entity
(e) See generally "**AXN Business Framework – Compliance Requirements and Regulations** within this document
(f) See generally "**AXN Business Framework – AXN Trustmark** within this document
(g) See generally "**AXN Assessor/Certification Framework**" within this document

23. Service Suspension Rights And Obligations
(a) Rights of APs and AXN Provider to suspend services

24. Termination Rights

(a) Rights of APs and AXN Provider to terminate services

25. Insurance Requirements

26. Procedures For Changes To Operating Rules

27. Miscellaneous Legal Provisions

(a) Relationships among parties

(1) Fiduciary relationship, if any
(2) Agency, independent contractor, joint venture, partnership, or trust relationship
(3) What about Cross borders transaction

(b) Dispute resolution issues

(1) Litigation, arbitration, mediation
(2) Mediation rules applicable
(3) Arbitration rules applicable
(4) Relationship to underlying substantive dispute between the parties

(c) Governing law/choice of forum

(1) Specify laws to govern the transactions
(2) Consider whether governing law will vary across transactions

Timeline/Evolution of AX Legal Issues

In the current AX ecosystem, risk allocations typically occur as follows:

- Limited or no AP liability for data accuracy or fitness for a particular purpose
- The AXN is responsible for data delivery/exchange, but not data accuracy or data reliability
- RPs, APs and AXNs are responsible for their respective data protection and privacy obligations

As the ecosystem evolves, these allocations may shift. For example as an AXN creates a more competitive market for attribute verification, APs may react by offering guarantees of accuracy of certain data verification types. It is doubtful that warranties of fitness for a particular purpose would be offered, as the RPs will be in the best position to decide the fitness of the data type for their use cases.

Within a trust framework, the goal of having the AXN serve as a contractual hub (whereby all RPs sign a contract with the AXN which includes flow down terms from APs) is more readily achievable than it is outside of a trust framework, where use cases are more likely to vary broadly. The goal of having a standard RP contract with the AXN as the hub may also morph as the market evolves.

Currently attribute verifying APs are strictly adhering to a “one bite at the apple” that prohibits RPs from vouching for the verified PII for another RP. Within a trust framework, the market may evolve to a point where APs are willing to allow RPs to share the verification, subject to a fee. The sharing fee could also be offered via an AXN and a competitive market for such data sharing would evolve.

Attribute Exchange Technology Framework

The AXN provides a foundation to address interoperability barriers that have impeded the full realization of the Identity Ecosystem. The AXN promotes user trust, security, and privacy by participating in auditable industry-established Trust Frameworks and Protocols as embodied by: the Open Identity Exchange (OIX) and Kantara; User-Managed Access (UMA); OAuth; OpenID; OpenID Connect; SAML; Cross-Origin Resource Sharing (CORS); and System for Cross-Domain Identity Management (SCIM) in addition to existing Internet security and transmission protocols. (See Appendix D for other protocols). Documentation of the technical architecture of this framework is divided into two sections.

Section One, an executive overview, terms of reference and other summary information is included within the main part of this document.

Section Two, the Technical Implementer's Guide (TIG) is a both a complete document but also included in its entirety as Appendix D to this document. The TIG is a stand-alone reference intended for use by technical, protocol and security architects who would be responsible for designing or implementing an instance of this framework.

Attribute Exchange Network Architecture

This section describes a distributed architecture that can be used to share critical information about a user between multiple parties. This architecture strives to use standardized mechanisms for trust between parties and to illustrate, at a protocol level, the scopes, tokens, and consent required. This section provides the technical underpinnings of an instance of an attribute exchange network and covers protocol level interaction and trust mechanisms required to pass attribute data.

Technical Description

The AXN architecture uses standardized mechanisms to promote trust between parties, to illustrate the data flows such as the scopes, tokens, and consent required at a protocol level. The following roles are defined for interaction with an AXN:

1. ***User Agent:*** The user is expected to operate an agent that is capable of receiving and processing HTTPS protocol requests, such as redirections that convey header information to and from other parties. The most common user agent is a browser.
2. ***Relying Party (RP):*** The RP is the protocol entity wishing to consume verified attributes. Usually the consumption of verified attributes is initiated by some user action such as a request for access to services.
3. ***Identity Provider (IDP):*** The IDP is the protocol entity that collects and asserts a persistent identifier (e.g., an OpenID credential) on behalf of the user. The IDP is responsible for protecting the integrity of this identifier and all tokens, scopes, attributes and consent exist relative to that identifier.
4. ***Attribute Provider (AP):*** An AP is the protocol entity that wishes to provide verified information about a user. The AP may not have any direct relationship to the end user.
5. ***Attribute Exchange Network (AXN):*** The AXN is the protocol entity that acts as a transaction and claims manager, interacting with all the protocol entities to ensure that user-asserted attributes are securely verified by participating APs, attribute claims from the AP are delivered with the user-asserted attributes to the RP, all with the consent of the user and all with the context of an identity that is asserted by an IDP. The AXN also collects revenues and distributes payments on behalf of network participants in accordance with the AXN business model, and provides a user interface whereby users can manage the distribution of verified attributes. The AXN does not store user attribute information, but uses an OpenID credential as an account reference key.

Participants of the OIX AXWG Legal Group

- Pamela Dingle, Ping Identity
- George Fletcher, AOL
- John Bradley, Ping Identity

- Chris Donovan, ID Data Web
- Ravi Batchu, ID Dataweb
- Amine Rounak, AOL
- David Coxe, ID Dataweb
- Scott Rice, PacificEast
- Peter Clark, Verizon

Goals

The overall goal of an attribute exchange network is to make verified attributes available to a Relying Party,with the participation and consent of an end user, as supervised and validated by that end user's Identity Provider. Verified attributes may be verified by one or more attribute providers, but are all linked to a single identifier published by an Identity Provider that has a strong existing relationship with the Subject.

High Level Steps

A succession of browser redirects and API requests are required to request access, verify consent, and communicate information between attribute exchange network parties.

User Redirections

Happy Path User Redirection

Figure 19 shows browser redirections in a successful attribute exchange, in the case where the subject already knows and consents to let both the AXN and the Relying Party work with the Identity Provider to exchange attributes. Note that solid arrows represent browser redirections, while dotted lines represent server-to-server API calls; and, the final API call to the AXN Verified Attribute API is shown below even though it is not a browser-based redirection to show the final step of retrieving actual attributes.

The steps shown in Figure 19 are as follows:

1. **Identity Assertion Request**
   A request made by the Relying Party to the Identity Provider to ascertain the identity of the subject and to obtain consent for the Relying Party to interact with the Identity Provider Valentine API.
2. **Identity Assertion Response**
   On successful authentication and authorization of the Relying Party, an OAuth 2.0 access token (AT1) will be returned to the Relying Party that can only be used by the Relying Party to query the trust list for the authenticated subject and to generate Valentine tokens for AXNs that are in the trust list.
3. **Locator Request with Valentine token**
   The Relying Party redirects the subject's browser to the AXN, including the Valentine token.

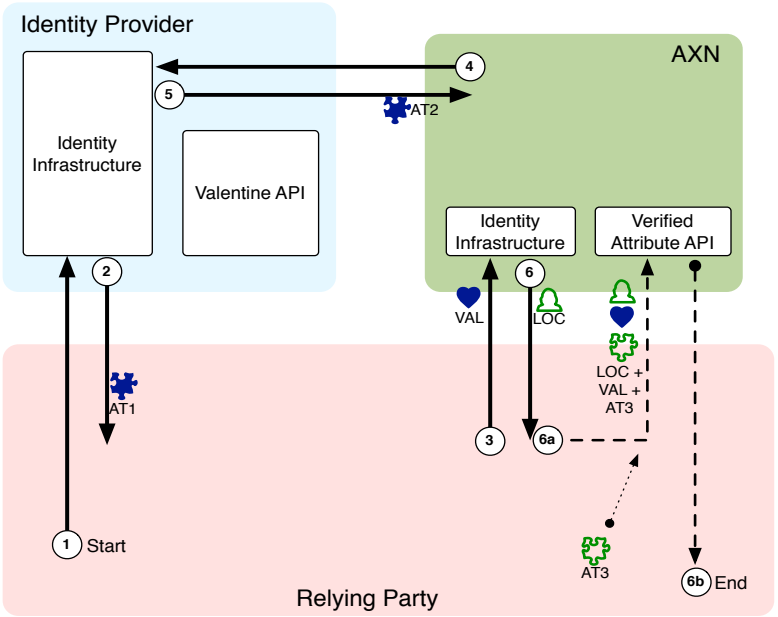


Figure 16: Happy Path Attribute Exchange with Browser Redirections

4. **Identity Assertion Request**
   A request made by the AXN to the Identity Provider to ascertain the identity of the subject and to obtain consent for the AXN to interact with the Identity Provider Valentine API.
5. **Identity Assertion Response**
   On successful authentication of the subject and authorization of the AXN as a trusted client within the attribute exchange context, the Identity Provider issues to the AXN an OAuth 2.0 access token (AT2) that can only be used by the AXN to update the trust list of the authenticated subject with AXN information and to validate Valentine Tokens for the authenticated subject.
6. **Successful Locator Response**
   The AXN redirects the subject's browser to the Relying Party, returning a locator to the Relying Party that can be used to access the AXN Verified Attribute API for this particular interaction.
   a. **Verified Attribute API Request**
   The Relying Party uses the locator in conjunction with the Valentine token and optionally a pre-configured API access token (AT3) in a server-to-server API request to the AXN to retrieve the verified attributes.
   b. **Verified Attribute API Response**
   Actual verified attributes are returned to the Relying Party.

Happy Path User Redirection with Valentine API Calls

In addition to the final server-to-server "back-channel" API calls that are documented above, additional back-channel calls are made from the Relying Party to the Identity Provider and from the AXN to the identity provider to determine whether a given AXN is trusted by the subject, and request a Valentine token representing the subject (on the part of the Relying Party) or to update the subject's trust of an AXN and validate a presented Valentine token (on the part of the AXN). Figure 20 shows all of the front-channel (solid line) browser redirections and the back-channel (dotted line) API requests and responses that occur in the happy path case where the subject already trusts the AXN prior to the beginning of the flow.

1. **Identity Assertion Request**
   A request made by the Relying Party to the Identity Provider to ascertain the identity of the subject and to obtain consent for the Relying Party to interact with the Identity Provider Valentine API.
2. **Identity Assertion Response**
   On successful authentication and authorization of the Relying Party, an OAuth 2.0 access token (AT1) will be returned to the Relying Party that can only be used by the Relying Party to query the trust list for the authenticated subject and to generate Valentine tokens for AXNs that are in the trust list.
   a. **Valentine API Requests**
   The Relying Party must first ascertain whether the currently authenticated subject already trusts the AXN and then must request a valentine token for the AXN (specific to the subject)
   b. **Valentine API Response**
   In the case that the subject trusts the specified AXN, a valentine token will be generated for that AXN and returned to the Relying Party.
3. **Locator Request with Valentine token**

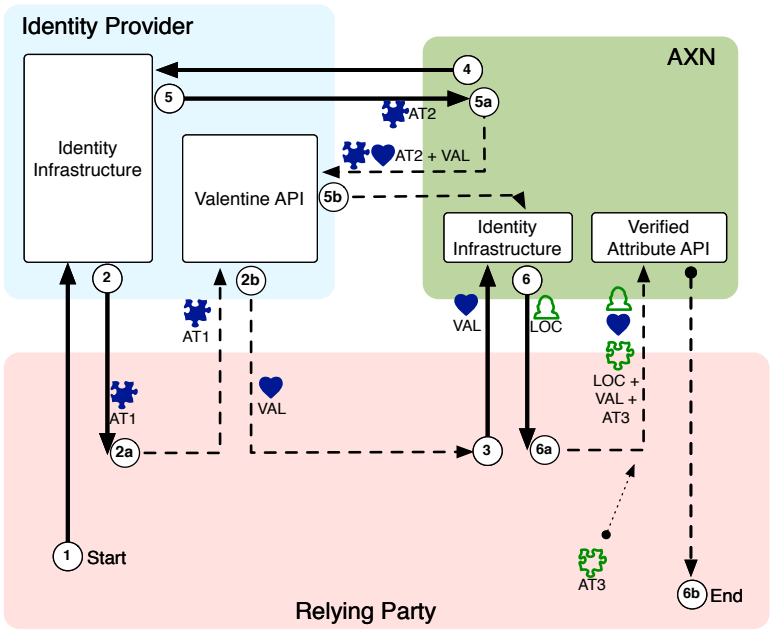


Figure 17: Happy Path Attribute Exchange with Redirects and API Calls

The Relying Party redirects the subject's browser to the AXN and includes the valentine token in the request.

4. **Identity Assertion Request**
   A request made by the AXN to the Identity Provider to ascertain the identity of the subject and to obtain consent for the AXN to interact with the Identity Provider Valentine API.
5. **Identity Assertion Response**
   On successful authentication of the subject and authorization of the AXN as a trusted client within the attribute exchange context, the Identity Provider issues to the AXN an OAuth 2.0 access token (AT2) that can only be used by the AXN to update the trust list of the authenticated subject with AXN information and to validate Valentine Tokens for the authenticated subject.
   a. **Valentine API Token Validation Request**
      The AXN submits the valentine token along with the AT2 access token to the Valentine API.
   b. **Valentine API Response**
      The Identity Provider checks that AT2 represents the same subject as the valentine token and is targeted for the same client, the AXN. If this is true a positive validation result is returned.
6. **Successful Locator Response**
   The AXN redirects the subject's browser to the Relying Party, returning a locator to the Relying Party that can be used to access the AXN Verified Attribute API for this particular interaction.
   a. **Verified Attribute API Request**
      The Relying Party uses the locator in conjunction with the Valentine token and optionally a pre-configured API access token (AT3) in a server-to-server API request to the AXN to retrieve the verified attributes.
   b. **Verified Attribute API Response**
      Actual verified attributes are returned to the Relying Party.

User Redirection Steps for Unknown AXN

In the case where a subject does not have a pre-existing relationship with an AXN, the Relying Party has to redirect the subject to the AXN without a valentine token to create a relationship with the Identity Provider, and then the AXN must redirect the subject back to the Relying Party to generate a valentine token and then initiate an API request to the AXN for the verified attributes.

The steps shown in Figure 21 are as follows:

1. **Identity Assertion Request**
   A request is made by the Relying Party to the Identity Provider to ascertain the identity of the subject and to obtain consent for the Relying Party to interact with the Identity Provider Valentine API.
2. **Identity Assertion Response**
   On successful authentication and authorization of the Relying Party, an OAuth 2.0 access token (AT1) will be returned to the Relying Party.
3. **Empty Locator Request**
   The Relying Party redirects the subject's browser to the AXN, but cannot include the Valentine token, because the AXN is not yet trusted by the subject.
4. **Identity Assertion Request**

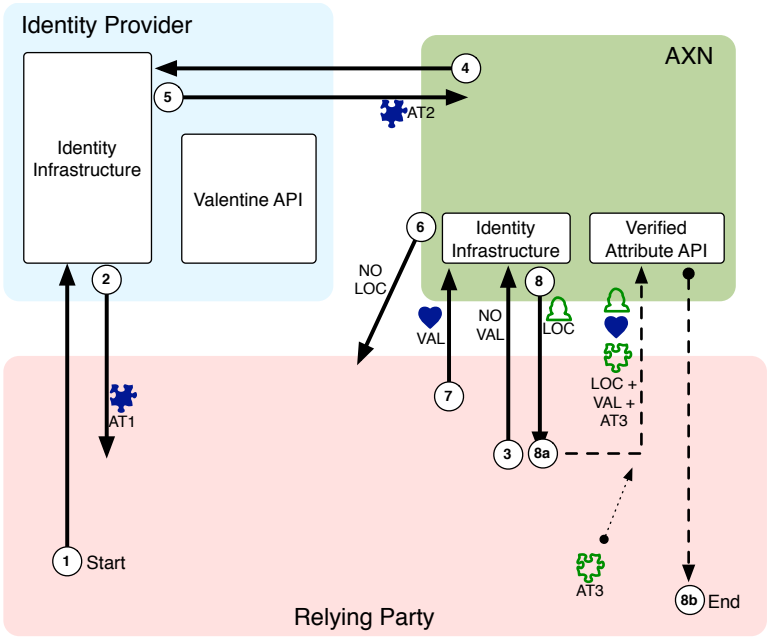


Figure 18: Unknown AXN Attribute Exchange with Browser Redirects

A request is made by the AXN to the Identity Provider to obtain consent for the AXN to interact with the Identity Provider Valentine API.

5. **Identity Assertion Response**
   On successful authentication of the subject and authorization of the AXN as a trusted client within the attribute exchange context, the Identity Provider issues to the AXN an OAuth 2.0 access token (AT2)
6. **Empty Locator Response**
   The AXN redirects back to the Relying Party without a locator, so that the Relying Party can now fetch a Valentine token.
7. **Locator Request with Valentine token**
   The Relying Party can now request a valentine token that is targeted to the AXN on behalf of the subject. The Relying Party again makes a Locator Request, this time including the valentine token.
8. **Successful Locator Response**
   The AXN can now validate the valentine token and redirects the subject's browser to the Relying Party, returning a locator to the Relying Party that can be used to access the AXN Verified Attribute API for this particular interaction.
   a. **Verified Attribute Request**
      The Relying Party uses the locator in conjunction with the Valentine token and optionally a pre-configured API access token in an API request to the AXN for the verified attributes.
   b. **Verified Attribute Response**
      Actual verified attributes are returned to the Relying Party.

User Redirection Steps for Unknown AXN with API Calls

The full set of redirection steps and API calls are diagrammed below but the steps are not spelled out, as they are very similar to the steps shown in previous sections. The steps shown in Figure 22, below, are as follows:

1. **Identity Assertion Request**
   A request is made by the Relying Party to the Identity Provider to ascertain the identity of the subject and to obtain consent for the Relying Party to interact with the Identity Provider Valentine API.
2. **Identity Assertion Response**
   On successful authentication and authorization of the Relying Party, an OAuth 2.0 access token (AT1) will be returned to the Relying Party.
   a. **Valentine API Requests**
      The Relying Party asks for or queries the subject's Trusted AXN List
   b. **Valentine API Responses**
      The list or answer returned from the Identity Provider indicates that this particular AXN is not yet known/trusted by the subject.

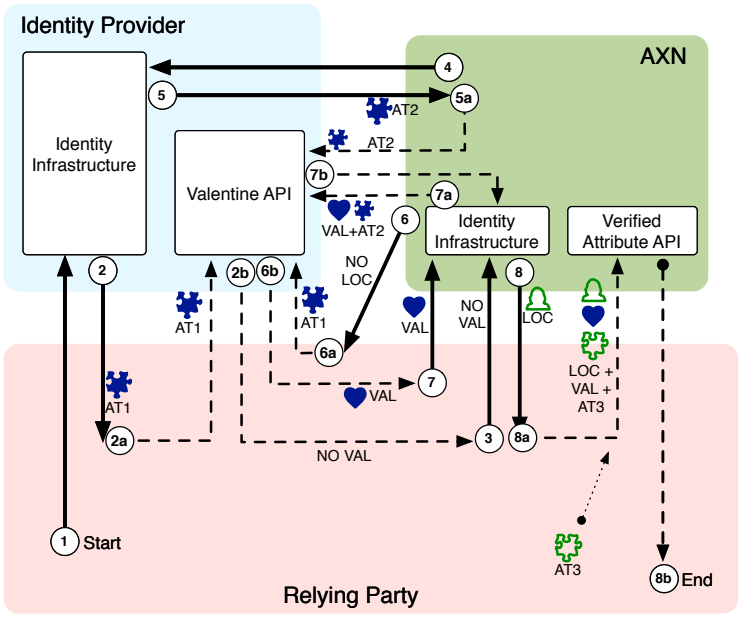


Figure 19: Unknown AXN Attribute Exchange with Browser Redirects and API Calls

3. **Empty Locator Request**
   The Relying Party redirects the subject's browser to the AXN, but cannot include the Valentine token, because the AXN is not yet trusted by the subject.
4. **Identity Assertion Request**
   A request is made by the AXN to the Identity Provider to obtain consent for the AXN to interact with the Identity Provider Valentine API.

5. **Identity Assertion Response**
   On successful authentication of the subject and authorization of the AXN as a trusted client within the attribute exchange context, the Identity Provider issues to the AXN an OAuth 2.0 access token (AT2)
   a. **Valentine API Requests (Trust List Insertion)**
      The AXN uses the AT2 access token to update or insert themselves into the subject's Trusted AXN List, thus enabling the Identity Provider to generate Valentine tokens.
6. **Empty Locator Response**
   The AXN redirects back to the Relying Party without a locator, so that the Relying Party can now fetch a Valentine token.
   a. **Valentine API Request(s)**
      The Relying Party again queries the subject's trusted AXN list and finds the AXN in the list. A Valentine token is requested.
   b. **Valentine API Response(s)**
      The Identity Provider returns a valentine token to the relying party.
7. **Locator Request with Valentine token**
   The Relying Party can now request a valentine token that is targeted to the AXN on behalf of the subject. The Relying Party again makes a Locator Request, this time including the valentine token.
8. **Valentine API Token Validation Request**
   The AXN submits the valentine token along with the AT2 access token to the Valentine API.
9. **Valentine API Response**
   The Identity Provider checks that AT2 represents the same subject as the valentine token and is targeted for the same client, the AXN. If this is true a positive validation result is returned.
10. **Successful Locator Response**
    The AXN can now validate the valentine token and redirects the subject's browser to the Relying Party, returning a locator to the Relying Party that can be used to access the AXN Verified Attribute API for this particular interaction.
    a. **Verified Attribute Request**
       The Relying Party uses the locator in conjunction with the Valentine token and optionally a pre-configured API access token in an API request to the AXN for the verified attributes.
    b. **Verified Attribute Response**
       Actual verified attributes are returned to the Relying Party.

Participation Requirements

Each participant has responsibilities in this system:

Identity Provider

- Must maintain an manage a "trusted AXN list" that represents the subject's relationship with one or more AXNs
- Must offer an API allowing a client to do the following:
  - Fetch a list of the subject's trusted AXNs
  - Fetch a valentine token intended for an AXN on the trusted list
  - Validate a valentine token
  - Update the trusted AXN list
- Must ensure that the user in some way knows and consents to allow a given participant to do any of the above activities

Relying Party

- Must have an existing relationship with one or more AXNs
  - Establishment of relationship is out of scope
- Must act as a relying party to make Identity Assertion Requests and validate Identity Assertion Responses from the IDP.
  - This may require a pre-existing relationship
- Must be able to interact as a client with the IDP Valentine API
  - To request "read" access to trusted AXN list and access to request valentine tokens

  - To parse the list and determine whether any AXN on the list matches an AXN that the RP has a relationship to
  - To request a valentine token for that AXN
  - To pass the token onto the AXN
- Must be able to interact as a client with AXN APIs
  - To trigger a request for verified attributes
  - To authenticate and securely retrieve verified attributes

AXN

- Must have an existing relationship with one or more Relying Parties.
- Must act as a relying party to make Identity Assertion Requests to the IDP and validate Identity Assertion Responses from the IDP.
  - This may require a pre-existing relationship
- Must be able to interact as a client with the Identity Provider Valentine API.
  - To request permission to update trusted AXN list and validate valentine tokens
  - To call the valentine validation API
  - To update the subject's trusted AXN list
- Must be able to issue a Locator which can be used to fetch verified attributes for the given subject and optionally within a given session context.
- Must offer an API allowing an RP acting as a client to do the following:
  - Request verified attributes
  - Fetch verified attributes

Constraints and Limitations

- Consent is narrowly defined in this document to mean protocol level consent. This means that the subject is authorizing a client or relying party to interact with an Authorization Server or Identity Provider.
  - Some Identity Provider APIs also collect consent for attributes to be passed in federated identity tokens.
  - Consent for release of identity data beyond what is offered by the IDP is the full responsibility of the AXN and is out of scope of this document
- Communication between the AXN and Attribute Providers is expected to be proprietary and is out of scope of this document.
- Note that it is not required that each IDP and AXN publish identical APIs or use identical federated identity methodologies. Participants must simply provide equivalent functionality that is sufficiently secured, such that the sequence diagrams can occur.
- New participants are encouraged to closely follow API examples provided in the Technical Implementer's Guide in the hope that a de facto API standard will evolve

Operational Recommendations

While not a part of the protocol level interactions, the following recommendations are necessary for full certification of the trust framework specification

Security Considerations

User identity security is foremost in importance; a core objective is to reduce the opportunities for identity misuse on the Internet while enabling users to manage how their information is used by IDPs and RPs on the Internet. The AXN leverages a number of standard protocols across a secure Hypertext Transfer Protocol Secure (HTTPS) network connection. These include:

- **Whitelist,** is a list or register of entities that, for one reason or another, are being provided a particular privilege, service, mobility, access or recognition. All RPs, APs and IDPs that participate with the AXN are whitelisted, to ensure only authorized businesses are passed user verified claims.
- **User-Managed Access (UMA),** is a web-based access management protocol designed to give a web user a unified control point for authorizing who and what can get access to their online personal data (such as

identity attributes), content (such as photos), and services (such as viewing and creating status updates), no matter where all those things live on the web.

- **Cross-Origin Resource Sharing** (**CORS**) is a web browser technology specification that defines ways for a web server to allow its resources to be accessed by a web page from a different domain.
- **System For Cross-Domain Identity Management (SCIM**) is a standard created to simplify user management in the cloud by defining a schema for representing users and groups and a REST API for all the necessary CRUD operations. In computer programming **create, read, update, and delete** (**CRUD**) are the four basic functions of persistent storage.
- **REpresentational State Transfer** (**REST**) is a style of software architecture for distributed systems such as the World Wide Web. REST has emerged as a predominant Web service design model.
- **OpenID** is an open standard that describes how users can be authenticated in a decentralized manner, eliminating the need for services to provide their own ad hoc systems and allowing users to consolidate their digital identities. Users may create accounts with their preferred OpenID IDPs, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication. The OpenID standard provides a framework for the communication that must take place between the identity provider and the OpenID acceptor (the RP) An extension to the standard (the OpenID Attribute Exchange) facilitates the transfer of user attributes, such as name and gender, from the OpenID identity provider to the relying party (each relying party may request a different set of attributes, depending on its requirements).
- **Open Standard For Authorization (OAuth)** allows users to share their private resources (e.g.,photos, videos, contact lists) stored on one site with another site without having to hand out their credentials, typically supplying username and password tokens instead. Each token grants access to a specific site (e.g., a video editing site) for specific resources (e.g., just videos from a specific album) and for a defined duration (e.g., the next 2 hours). This allows a user to grant a third party site access to their information stored with another service provider, without sharing their access permissions or the full extent of their data.

A user's PII will not be stored at the AXN, but will be under direct user control via the user's Personal Data Service (PDS) at an online location of the user's choice. The user will assert their attributes at RP sites to establish an account and procure services, and after completing their first verification flow, the user can easily leverage verified attributes to establish new RP accounts, thereby minimizing user friction and promoting adoption. Throughout this identity ecosystem, the user will be leveraging a credential (e.g., OpenID) issued and managed by their IDP, which minimizes the use of passwords and reduces the friction associated with user account creation and log in.

The AXN design mitigates many potential threats by virtue of not creating a central data store of verified user attributes. In addition, security and privacy enhancing and protecting technology is built into the AXN infrastructure as follows:

- The implementation of AXN data flows uses Oauth 2.0, HTTPS for the transport layer, white lists to only allow registered IDPs, APs, RPs and users to access the AXN, and encryption techniques applied to data at rest
- OpenID is used for user credentials, AXN user account creation, and user access to the AXN is restricted to being available only via the user's registered IDPs and RPs
- User opt-in to each process control step associated with data collection, verification, and distribution of user attributes
- The use of out of band user verification methods (in addition to an IDP-issued OpenID) by the AXN to authenticate users as they access the AXN using their OpenID (only from IDPs and RPs registered with the AXN) such as SMS with a PIN, IP address, registered device ID, Biometric technologies, and Knowledge Based Access (KBA)
- The AXN user attribute data exchange with IDPs is limited to an encrypted token indicating that an attribute was verified and available with user consent via the AXN to participating RPs; and the actual verified user attributes are not provisioned directly to participating IDPs by the AXN
- Transport Layer Security (TLS) enables a secured connection, which is encrypted and decrypted with key material until the connection closes to prevent data eavesdropping and tampering.

Users will authenticate to their IDP to use their OpenID credential before initiating an account login with their RP. The AXN will create an account for each user, and will accept the OpenID credential as provisioned by the IDP.

The AXN will also implement various verification services and methods that will generate claims associated with each user attribute. In all cases, participating RPs will consume the user asserted, verified attributes and associated claims to implement user authentication and authorization services prior to provisioning a user account and user access.

Application Hosting and Infrastructure

As a cloud service, the AXN doesn't require external systems to be provided by the customer for standard operations. Any RP or IDP specific requirements for security or privacy should be readily accommodated. The AXN is designed to evolve and be maintained using standard software development methodologies. Any new requirements will be implemented as needed based on a thorough understanding of the customer requirements that are subsequently further refined into functional specifications for product development.

The AXN is designed to scale as needed. Resources are dynamically allocated based on loading requirements with expected uptime of 99+%. If the attributes are being verified for the first time, the entire verification flow can take between 2-3 minutes based on user response time. If the attributes are already verified by user for a different RP, it can be less than 10 seconds.

Additional Technical Details

Detailed description of transactional flows, scope, tokens, specific responsibilities of each party and example use cases and scenarios are provided in the Technical Implementer's Guide (Appendix D). The TIG provides sections and details for the following:

- Identity Provider Valentine API Requirements
- Identity Provider Valentine API Authentication
- Verified Attribute API Requirements
- Verified Attribute API Authentication
- AXN Locator Request & Response
- Detailed Protocol Sequences
- Design Pattern Recommendations
- Special Appendices of Examples

AXN Privacy Policy Framework

Introduction and Background

The **AX Privacy** specifications are designed to ensure the Internet Identity Ecosystem is user-centric, meaning each individual user will have more control over the private information used to authenticate themselves online, and generally will not have to reveal more identity data than necessary to use the RP service. It is also critical that readers and implementers realize that this is NOT a US centric specification and that Attribute/Service Providers MUST operate according to the legal and regulatory requirements of the jurisdiction(s) in which they operate. The work of the AX Privacy/Policy Group has entailed the following activities:

- Identify the types and categories of user consent regarding the use of their personally identifiable information (PII). For example, the trust framework may provide the means for a user to opt-in to allow commercial transactions to be authorized, but perhaps not allow users to opt-out of fraud prevention techniques.
- Identify the OIX privacy criteria for attribute exchange in the context of existing principles:
    - Compare privacy principles of ICAM, EU, US Consumer Bill of Rights, UK and other countries (see Appendix B)
    - Coordinate with other AXWG working groups identified in this document to ensure that the privacy considerations are included in the overall trust framework model
- Develop the privacy criteria according to the legal and regulatory requirements of the legal jurisdiction in which the Service Provider operates:
    - Provide the **Individual control and consent** over the collection, use or disclosure of attributes
    - **Identify the purpose** of collection in easy to understand terms
    - Be **transparent and open** about your policies and practices for attribute exchange
    - **Limit the collection of attributes** to what is necessary for the purpose identified
    - **Provide the Individual with reasonable access** to the attributes that you collect and maintain
    - Provide the individual with **a means to terminate, suspend or change** the attribute data
    - Provide reasonable **safeguards** to protect the attributes under your control
- Coordinate with other entities in the identity management space to develop a coordinated path to support the broadest industry participation and user/consumer uptake.

Participants of the OIX AXWG Assessor/Certification Group

- Dale Rickards, Verizon, Identity, Regulatory Affairs, Audit and Compliance (Chair of the PPWG)
- Rich Furr, Verizon, Identity, Regulatory Affairs, Audit and Compliance
- Naomi Lefkovitz, NIST, NSTIC Senior Privacy Advisor
- Debbie Diener, Privacy Consultant
- Tom Smedinghoff, Edwards Wildman Palmer LLP
- Scott Rice, PacificEast, CIO/EVP
- Domenic DiLullo Accenture (formerly Department of Homeland Security)
- Michael Brody
- Peter Graham, Verizon
- David Coxe, ID Dataweb, CEO
- Nick Kalisperas

Attribute Exchange Privacy Criteria

The privacy criteria described below identify the fundamental guiding privacy principles for attribute exchange. If any of these privacy principles conflict with national or local privacy laws or regulations in the jurisdiction in which the Service Provider operates the local privacy laws and regulations take precedence.

User Control and Consent

Informed consent from the User is required for the collection, use, or disclosure of personal attributes. Users shall have a right to exercise control over what personal attributes and Service Provider collects from them and how they are used.

The User shall have the right to withdraw their consent to exchange attributes with a Service Provider at any time. The withdrawal of consent shall not affect the legality of the attributes exchanged prior to withdrawal of consent.

The User shall be able to see each attribute that a Service Provider transmits to a as part of an Opt-In consent process. Users shall be able to Opt-Out of providing User attributes to a Service Provider. This Opt-in/Opt-out function does not have to happen at the time of the transaction but can be part of a profile, which is managed by the User. If this has implications (e.g., that the User may not be able to access particular services, or that the User may not be able to access particular services online) this shall be made clear to the User.

Identifying Purpose

The Service Provider shall identify the purposes for which personal attributes are collected to the User in easy to understand terms at or before the time the information is collected and verified.

The User must be provided with a clear description that provides the details related to the processing of personal attributes in advance of any processing. The information provided must include a clear explanation of why the User must provide any specific attribute information (e.g., to confirm their identity before a bank loan is provided) and must also identify any obligation on the part of the User (e.g., in relation to the User's role in securing his/her own attribute information). Any subsequent change to the previously described processing arrangements shall require the User to provide updated consent before the change becomes effective. The User shall also be informed of the consequences of not providing updated consent.

Transparency and Openness

The Service Provider shall make specific information about its policies and practices relating to the management of personal attributes (e.g., privacy and security practices) readily available to Users.

The Service Provider should engender trust by being open about all aspects of the processing of personal attributes (Processing means "collecting, using, disclosing, retaining, transmitting, copying, comparing, corroborating, aggregating, accessing" and anything else).

Limiting Collection and Data Minimalism

The collection of personal attributes shall be limited to that which is necessary for the purposes identified by the Service Provider. Attributes shall be collected by fair and lawful means.

The personal attributes processed by a Service Provider to facilitate a request of the User shall be the minimum necessary in order to fulfill that request in secure and auditable manner. Service Providers shall limit the use and disclosure of personal attributes to those purposes that are consistent with both the relationship they have with the User and the context in which User originally disclosed the data, unless required by law to do otherwise. If Service Providers will use or disclose personal attributes for other purposes, they shall disclose these other purposes in a manner that is prominent and easily actionable by Users at the time of data collection. The User shall be provided an Opt-out option if they do not agree to a purpose of collection (e.g., The User could Opt-out of using their attributes for marketing purposes)

Service Providers shall transmit only those attributes that were explicitly requested by the Relying Party. The Relying Party must only request those attributes that are necessary for the transaction.

Data Quality, Accuracy and Access

Service Providers shall use reasonable measures to ensure they maintain accurate, complete and up-to-date attribute data. Service Providers shall also provide Users with reasonable access to personal attribute data that they collect or maintain about them. Users shall also have appropriate means and opportunity to correct inaccurate personal attribute data or request its deletion or use limitation.

Upon request, a User shall be informed of the existence, use, and disclosure of his or her personal attribute information and shall be given access to that information. A User shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Portability and Accountability

A Service Provider is responsible for attribute information under its control and shall designate a User or Users who are accountable for the organization's compliance with these privacy requirements. Each Service Provider must allow, promptly, on request and free of charge, each User access to any personal attribute data under its control that relates to that User.

Service Providers that disclose personal attribute data to third parties should, at a minimum, ensure that the recipients must comply with enforceable contractual obligations to adhere to these privacy requirements, unless they are required by law to do otherwise.

The Service Provider that controls the User's attribute data will provide Users a means to terminate, suspend or change the data.

Safeguards

Service Providers shall assess the privacy and security risks associated with their attribute data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.

There shall be a certification procedure subject to an effective independent audit regime, which ensures that all Service Providers meet or exceed the Attribute Exchange Trust Framework requirements and that all relevant and recognized technical standards, data protection and other legal requirements are maintained. In the context of attribute data, certification procedures should include the use of Privacy Impact Assessments and Privacy by Design concepts.

Challenging

Each Service Provider shall provide a means for an User to be able to address a challenge concerning compliance with the above principles to the designated User or Users accountable for the attribute data exchange compliance within their organization.

AXN Operational Privacy Principles – An Example

The AXN attribute exchange mechanisms provide APs with an interface to register AP attribute verification service offerings via the AXN (including attribute type, data type, coverage, refresh rate, currency, pricing and contract type) which when coupled with AXN out of band methods generates a service pick list from which RPs can select to satisfy their Use Case requirements. The Attribute services that ultimately may be made available via an AXN may include name, email, address, telephone number, date of birth, gender, full or partial SS number, picture, device ID, CAC, PIV, etc., but will be limited to those required by an RP for a permissible purpose to provision a user account and grant access to the RP service. The Terms of Service for participating RPs should include rules regarding re-use and distribution by RPs of user attribute data as provisioned via the AXN. Enforcement and audit of these RP Terms of Service will be subject to the industry-specific legal and regulatory constructs and the policies embodied in the corresponding implementation of the AX Trust Framework.

The AXN collection and payment system must identify transactions by transaction IDs, and only where required by trust framework policy, user credential and local database references appropriate for each participating IDP, AP and RP. By using transaction IDs, the user-asserted and verified attribute data should only be referenced in the abstract in the collection and payment system.

In the US, the Fair Information Practice Principles (FIPPs) are the basis of the AXN's privacy compliance policies and procedures governing the use of PII. These principles are embodied in the implementation of the AXN service infrastructure with a community of IDPs, APs and RPs in the user interface, disclosure statements, terms of service, data flows and data handling components. The implementation of some principles may vary depending upon the corresponding business, legal, technical, privacy/policy and assessor/certification requirements specified in a given Trust Framework. More specifically, the AXN should enable the following:

- User interfaces that are transparent and provide notice to the User regarding the collection, use, dissemination, and maintenance of PII;
- Active user participation in PII use, seeking user consent for the collection, dissemination, use, and maintenance of PII, and providing mechanisms via the User Accounts interface for appropriate access, correction, and redress regarding use of PII;
- Specifically obtain user permission for the collection of PII and specifically articulate the purpose(s) for the intended use of the PII;
- As specified for a given Trust Framework, only collect PII that is directly relevant and necessary for the RP to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s);

- Use PII solely for the purpose(s) specified in the notice, and sharing PII outside the AXN and related Trust Framework is only with user permission and for a purpose compatible with the purpose for which the PII was collected;
- To the extent practicable, actively engage participating APs, IDPs, and the user with a portfolio of attribute verification and trust elevation services to ensure that PII is accurate, relevant, timely, and complete;
- Protect PII through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure;
- Be accountable for complying with these principles, providing training to all participants who use PII, and be subject to audit for the actual use of PII to demonstrate compliance with these principles, all applicable privacy protection requirements, and any requirements specified in a corresponding Trust Framework.

The AXN should employ a customizable, use-case specific set of user interface templates and transaction flows that initiate when a user desires to create an RP service account using a login credential from the user's IDP. The user must first login with their IDP, and then give permission to the IDP to share user account information with the RP and the AXN. The RP then notifies the user that additional information must be verified to create a new RP account, the user opts-in to have their information verified by the AXN (per FIPPS as described above), and then opts-in for their user asserted, verified attributes to be shared with the RP. APs on the AXN only verify user attribute claims, and do not provision user attributes to or via the AXN. The RP uses the verified user attributes (with user permission) to authenticate the user, create a user account, and authorize the user to access the RP service. The RP site publishes a "verified account" status with a link back to the AXN User Accounts page that displays a list of verified user attributes and where the user can update changes to their attribute assertions. Once verified, updated attribute claims will be published to the participating user RPs. At this site, the user can also view and change/delete the attributes shared with each of their RPs. The user's IDP obtains (with user opt-in) a token from the AXN signifying that verified user attributes and claims are available via the AXN, but user attribute information is not shared with the IDP. The token is also used to update the IDP User Account page where the user can revoke access for a given RP to the user's IDP account.

The privacy obligations among the participants associated with user transaction aggregation/correlation are subject to the policies of the corresponding Trust Framework. The AXN user account relationships are user managed, and user transaction data is not correlated or released in aggregate to participants. APs contract directly with the AXN for providing verified attribute claims for user-asserted attributes, and do not have access to RP-specific transaction data, unless required for audit or by a Trust Framework.

The AXN provides a market effective methodology for APs and RPs to determine the data required and the best value to all parties based on their business needs. Additionally, the trust framework provides a set of standards for minimum acceptable practice for all parties. AXN policy may include:

- Data Minimization: Participants that use PII or sensitive user information for online behavioral advertising may be required to obtain opt-in consent; however, opt-out consent is required for the use of non-sensitive, non-PII. In the US, the policy may also extend the Children's Online Privacy Protection Act to non-PII and require verifiable parental consent for any use of non-PII to create an interest segment for behavioral advertising that is specifically targeted to children under the age of 13. In addition, the policy may require participants to retain data collected for online advertising purposes for the length of time required to fulfill a legitimate business need.
- Use Limitation: The Network Advertising Initiative (NAI) Code provides that members may only use, or allow the use of, consumer interest segments for marketing purposes.
- Data Quality and Integrity: AXN and its participants will make reasonable efforts to ensure that they obtain data for uses from reliable sources.
- Security: Members may be required to provide reasonable security for the data they collect, transfer, and store for online advertising purposes.
- Accountability and Auditing: AXN participants may be required to publically attest to compliance with the policy, and these attestations are subject to FTC enforcement. Members may be also required to undergo annual compliance reviews. The results of the compliance review and a summary of consumer complaints are required to be published annually.

AXN Assessor/Certification Framework

Attribute exchange and identity management technologies hold promise to reduce the friction of using the Internet, but they are not usually sufficient to address the question: Whom do you trust? In other words, how does a relying party know it can trust credentials from an identity service provider without knowing if that provider's security, privacy, and operational policies are strong enough to protect the relying party's interests? How does a user know if the identity providers and relying parties can be trusted to protect sensitive personal information, abide by the user's preferences and protect the user's privacy? And, all parties want to know if the practices described by the other parties are actually those implemented, and they want to verify the reliability of those parties.

The OIX AX Trust Framework, like other Working Group efforts, is designed to help specific implementations get started by a given community of interest (COI). Generic certification profiles may be useful to a wide range of implementations of an AX Trust Framework. Auditors, assessors, certifiers may rely on OIX WG trust framework documentation to help develop COI certification requirements for auditors, assessors, and other participants.

Participants of the OIX AXWG Assessor/Certification Group

- Ray Kimble, Deloitte
- Myisha Frazier-McElveen, Deloitte
- Dan Combs, eCitizen Foundation,
- Sarbari Gupta, Electrosoft
- Nathan Fault, KPMG
- David Coxe, ID DataWeb
- Sal D'Agostino, IDmachines

AXN Assessor/Certification

The Assessor/Certification section of the OIX AX Trust Framework provides important high level guidance. The true test and success of any trust framework is its function in the market: and the perception of participants of its operational integrity and ultimately in its adoption. While the OIX Board approval of a Trust Framework does not require an Assessor/Certification component, it does require an evaluation of whether it comports with OIX's principles of openness. As such, the AXWG has elected to provide appropriate guidance as each implementation is by definition unique, and each may require assessments to provide business, legal or technical value.

Risk adverse markets often start with a need for an external reference or certification regime for each actor in the trust framework (e.g., IDP, AP, RP and importantly the end user). The important role of accreditation, certification, and audit in these sectors (e.g., government, financial services, etc.) will continue. Government, industry and academia market a range of certifications, assessments, audits and other risk management processes. COIs that reference OIX trust framework templates will ultimately succeed based on the desire for cost effectiveness, operational efficiencies and risk management. Those that yield limited, practical outcomes at scale or that have overly restrictive policies that increase friction will likely be marked by slow or little adoption.

Some early versions of certification for internet identity implementations have frustrated some market participants, large international players as well as small startups, given the expense, legal exposure and meager risk management value provided by some accreditation bodies. Some large IDP's have reasoned that should a breach, or other legal action occur, they would be the first, and last resort, for financial or brand damages. They note that many of those marketing compliance or certification services often have little real world technical expertise and operational experience in today's rapidly changing internet identity systems. They point out the lack of certification required in many high volume and velocity albeit low assurance commercial (identity-oriented) transactions. Many large IDP's have consistently pointed out that their willingness to commit their brands to compliance was more material than assurance provided by others.

There has been a clear consensus in the commercial market to focus on the need to make certification, accreditation and best practices more effective (e. g., more practically relevant in business, legal and technical terms). OIX is building OIXnet, an open Trust Framework Metadata Listing Service. The OIXnet Registry is intended to be an enabling platform as it allows those implementing a given trust framework to more easily connect and interoperate with other communities of interest, disclose their business, legal and policy requirements, and have the approach validated by its adherence to the "Principles of Openness" in its OIX registration.

AXN Auditing and Reporting

The AXN enables an online Attribute Exchange between market participants whereby APs post a listing of attribute verification services and RPs select the services that support their requirements. Each RP, IDP, AP, and user will be registered and provisioned a corresponding account on the AXN to support auditing and reporting. The exact auditing and reporting requirements will be determined as the AXN rolls out and will incorporate the level of auditing and reporting appropriate for a given Community of Interest (COI) from a business and technical perspective. As an example, it could include:

- RP management console so RPs can choose from a list of AP service options. A given RP might want a combination of services (e.g., Real-time AP services, plus Phone SMS, plus Phone call, plus TPM, etc.) and a menu of attributes per service (e.g., Name, Email, Address, Telephone, SS#, Gender, Age, TPM cert, PIV cert, CAC cert, etc.). This console may include RP account info such as contact info, billing method, preferred APs, and AXN contract info. An RP administration policy may also require the RP to specify the purpose and agree to data minimization as specified in the corresponding trust framework and as defined in the RP's legal agreement with the AXN. Each RP will also specify privacy principles, guidelines and/or policy similar to the current practice today and as specified by the trust framework for their COI.
- AP management console for APs to establish an account, manage monetization options (e.g., per transaction fees, periodic (quarterly, annual) subscription fees), review transaction logs, and ultimately, market exchange contracts (e.g., spot pricing formats for attribute verification services). As more APs engage on the AXN, a set of rules will evolve by which APs will be engaged by RPs when verifying user attribute assertions. For example, if a user can't be verified with their preferred AP, should the RP have the AXN try to verify with other APs before mailing a PIN code to the user's street address?
- IDP management console for IDPs to establish an account, manage monetization options (e.g., per transaction fees, periodic (quarterly, annual) subscription fees), review transaction logs, and ultimately, manage exchange contracts.
- AXN management console for the AXN – could present the participating IDPs, APs, RPs, operating stats, billing stats, reports, etc.:
    - AXN contract terms for each participant
    - AXN Attribute Processing and Provisioning (APP) for each AP account and service – essentially the AXN revenue distribution factors (Factor 1 and Factor 2) that will vary depending upon the list of items configured in the AP Management Console.
    - AXN UI automation database – pulling logos; custom AP picklist requirements for attribute types, etc. and publishing this data to the corresponding interfaces.
    - Reports – transaction audit logs, billing logs, payment logs (to APs and IDPs)

The audit capabilities on the AXN can be based on transaction logs and management console reports for each group of participants and leverage the transparency inherent in all aspects of the AXN. Basic AXN transaction logs would be available out of the box, and various capabilities for notifying participants have been identified as requirements for the AXN:

- User transaction notifications to those who elect to be notified
- IDP notifications about the status of whether a user's attributes have been verified

Users could manage the how their attributes are shared with RPs online via the user admin console. Additional reporting and notification functions could be implemented as the requirements are better defined for a given COI trust framework.

Summary, Lessons Learned and Conclusions

Summary

The Attribute Exchange (AX) Trust Framework specification is intended to enable what some call the "Identity Information Exchange Ecosystem." This is an ecosystem or marketplace that is interoperable, secure, privacy preserving, and allows users to share reliable identity information with service providers who wish to utilize them. The objective is to provide a starting point from which a Community of Interest (COI) can organize participation from their constituency to customize and implement the business, legal, technical, privacy, certification and audit components of their AX Trust Framework specification.

As defined herein, an Attribute Exchange Trust Framework is designed to enable trusted delivery of online identity as a service to participants with a scalable, secure, low-cost, and convenient solution. A framework consists of multiple parties whereby a user is issued a digital credential by a commercial identity provider (IDP), such as their bank, email or social network provider, with which they already have an online relationship. This credential is used to interact online with a service provider called a Relying Party (RP). RPs may in turn request additional information about a user that is satisfied by Attribute Providers (AP), after which RPs may authorize access rights to authenticated and verified users.

An Attribute Exchange Network (AXN) is an online Internet-scale gateway for IDPs and RPs to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs. The AXN standards-based platform deploys a business model that simplifies online identity verification for APs, RPs, and IDPs. This business model will ultimately reduce costs to RPs while generating revenue to APs and IDPs. The AXN is responsible for the processes and policies associated with establishing, maintaining, and distributing verified user identity attributes. AXN attribute maintenance includes validating, updating, and revoking attribute claims. An attribute provider on the AXN validates a user-asserted attribute claim and the AXN provisions that verified claim, with user permission, in response to attribute requests from RPs

The AXN's revenue model is based on a mutually beneficial business model, the composition and commitment of the existing industry participants, and the availability of public and private sector RPs. The AXN business model is critical to overcoming historical implementation barriers and expanding the participation of RPs through a mechanism for efficiently servicing and monetizing existing RP markets and new business currently underserved by existing online Identity Ecosystems. The AXN provides a means for APs to efficiently access and monetize their AP services to a large array of IDPs and RPs in global online markets. It is a neutral market channel optimized for open, competitive internet scale participation. It is also an online credential management and attribute exchange monetization platform – unencumbered by legacy business models, regulations and technologies.

AXN AP participants use the standards-based APIs and cloud-based, interoperable transaction AXN infrastructure to share revenue generated from RPs for purchases of verified user-asserted attributes. The AXN promotes user trust, security, and privacy by participating in auditable trust framework processes and policies, as exemplified herein. The AXN also expands the addressable market not currently supported by APs to include small and medium size RPs by enabling affordable access to verified user attributes via an online attribute exchange.

Agreements between all parties contractually enforce the business, legal, technology, policy, certification and audit aspects of the Trust Framework, which are established and managed by a Trust Framework Provider (TFP) via an AXN. When adopted across a broad range of IDPs and RP websites and applications, the Attribute Exchange Trust Framework provides a scalable solution for online user attribute exchange to enable higher levels of assurance, authentication and authorization at a lower cost and with greater convenience for users.

To support these objectives, an AX Trust Framework must specify a consistent, provider-agnostic set of information exchange protocols and policies for the purpose of facilitating attribute verification, digital identity management and fraud prevention that also preserve or enhance user privacy. These information exchange protocols and policies, or "rules and tools", allow for access to necessary user identity attributes as requested by an RP for a specific transaction without interfering in, risking, or devaluing the primary relationship between the user and the online community of RPs.

The AXN reference architecture enhances user privacy and control over their verified user attributes without creating a centralized data store of user attributes at the AXN. Throughout this identity ecosystem, the user will be

leveraging a credential (e.g., OpenID, SAML) issued and managed by their IDP, which minimizes the use of passwords and reduces the friction associated with user account creation and log in.

The Technical Implementer's Guide (TIG) addresses cases when the individual already knows and consents to have the AXN, RP and IDP cooperate to exchange the user attributes, and also for cases when the individual does not yet know about the AXN. The technical guidelines and design patterns provided represent the minimum requirements for a secure implementation. The implementation suggestions and lists of responsibilities have been outlined for each entity's role for both cases. Consideration was given to prevent requests for unauthorized information both from external sources and from rogue or unauthorized requests from within authorized entities.

An AXN will raise the level of confidence across the Identity Ecosystem by enabling the following services:

- Manage secure, one-to-many open standard-based APIs to connect all participants to the AXN infrastructure platform for data flows between APs, IDPs, and RPs
- Manage payment collections from RPs for verified attributes and distribute payments to APs and IDPs
- Manage standard legal contracts and appropriate Service Agreements (SAs) for attribute exchange on a one-to-many basis with IDPs, RPs, APs, and Trust Framework Providers (TFP), Assessors, and user Terms of Service (TOS)
- Support a user attribute management interface to enable user attribute opt-in/opt-out for each RP account relationship through an AXN user Admin Console, or support this service through the user's IDP
- Support policy compliance by ensuring the AXN collection, storage, release, transport, and use of user attributes with APs, IDPs, and RPs channels conforms with Trust Framework business, legal, technical, and privacy policy controls
- Manage transaction logs with AP, IDP, and RP channels in support of ongoing security, privacy and policy audit requirements as defined for each trust framework

While the overall objectives of an AX Trust Framework will include improving online user trust, privacy, and online security, the purpose of the OIX Attribute Exchange Trust Framework specification is to publish a practical roadmap for how a TFP can quickly implement a trust framework to address their specific market requirements. RP Use Cases and AXN reference architecture serve as the common foundation for the work group contributions included in this AX Trust Framework specification. The OIX AX Trust Framework Specification contained herein is a starting point from which each Community of Interest (COI) will need to organize participation from their constituency to customize the business, legal, technical, privacy, certification and audit components of their AX Trust Framework specification.

The COI **Business Group** should lead this effort by identifying industry sectors ideally suited for an AX Trust Framework and developing RP Use Cases, service definitions, monetization models, and high level requirements related to business, legal, and technical processes. Additionally, various Use Case models must be defined for establishing a TFP business entity for exchanging ownership, obtaining resources, and securing funding from industry participants and to define ongoing income streams to perpetuate trust framework operational requirements.

The COI **Legal Group** should deliver the legal portion of the AX Trust Framework Specification. As the AX Trust Framework specification evolves, a set of legally binding agreements should be implemented based on a common set of criteria to manage risk with the AXN serving as a contractual hub. The objective should be to deliver a set of legal agreements that are required to implement an active trust framework.

The COI **Technology Group** should deliver the technology, standards, data flows, and technical interface criteria for the AX Trust Framework specification based on the appropriate AXN reference architecture. Below is a high level list of topics that should be covered by the working group.

- Define risk mitigation requirements and a set of common operating rules appropriate for the portfolio of RP applications
- Identify supported transactions and transaction standards
- Identify supported information exchange protocols (e.g., OpenID, OpenID Connect, OAuth, SCIM, XML)
- Identify supported technical interoperability standards (e.g., OpenID, XUA, UMA, SAML, PKI)
- Identify supported APIs
- Develop models for data flows, data handling, and data caching

The COI **Privacy Policy Group** should be responsible for ensuring the Internet Identity Ecosystem is user-centric, meaning each individual user will have more control over the private information used to authenticate themselves online, and generally will not have to reveal more identity data than necessary to use the RP service. This Group

should, at a minimum:

- Identify the user permissions and categories of permissions. For example, the trust framework may provide the means for a user to opt-in to allow commercial transactions to be authorized, but perhaps not allow users to opt-out of fraud prevention techniques
- Identify the minimum privacy requirements that should be implement to provide protection for Personal Identifiable Information (PII) exchanged in the AXN.

The COI **Certification/Assessment Group** should be responsible for defining Assessor processes and qualifications, the certification requirements for trust framework membership, and the process for membership recertification. In general, an Assessor must provide written evidence that performing audits is a regular ongoing business activity, including tax filings showing a relevant industry code, financial statements showing a majority of revenue from compliance auditing, and a list of compliance audits performed in the past two years with contact information for verification.

Lessons Learned From Pilots

The AX Trust Framework specification was developed by OIX community participants some of whom were actively engaged in parallel pilot project activities using AXN reference architecture as defined herein. The feedback from ongoing pilots with IDPs, APs, users and RP customers provided valuable input to the evolution of the specification. The objective was to design a practical guide for how to implement operational business models for online attribute exchange. What follows is a summary of lessons learned from pilots that might prove useful in supporting the evolution of AX Trust Framework specifications:

- Emerging Trust Frameworks are being driven by Communities of Interest (COI) who seek market operational efficiencies through business, legal, technical and policy interoperability. RPs are the customer, and will drive market requirements, adoption, and policy controls. Credential federation using verified user attributes requires RPs to evaluate and change policy to enable significant security, user experience (SSO and account creation), and business benefits. RP business requirements must be clearly identified, and a marketing and messaging campaign for a COI may be required during the early stages of implementing a Trust Framework to engage participation.
- As a contractual and transaction hub, an AXN can greatly simplify how RPs access IDP and AP services. The AX Trust Framework contractual components are expected to simplify as the AXN business model is better understood and is generally accepted by market participants. The ultimate goal for a COI should be to implement one set of standard legal agreements that embody the business, legal, technical, privacy and audit requirements for that community.
- As defined herein, users opt-in to asserting attribute for verification by APs and subsequently provide permission for the sharing of their attributes (and related claims) with RPs. Having the user opt-in and actively engaged in the transaction meets many of the regulatory requirements inherent in traditional AP contracts. As such, related contractual terms should evolve quickly and simplify RP legal review as the market develops.
- RP risk mitigation strategies (for a required LOA per NIST SP 800-63) lack consistency and clear policy guidance. Trustmarks could be used as a means to provide consistent messaging and objectively promote confidence in various combinations of authentication methods. Emerging user-centric trust elevation technologies are scalable, cost effective and interoperable and provide a rich portfolio of options for risk management. Verified user attributes, and attribute claims from device identities, biometric technologies, can be used in combination with PKI and non-PKI technologies, including card-based solutions, to enable a broad array of risk mitigation options. A portfolio of risk mitigations solutions enables RPs to enable cost-effective federated credential login (to an account established with verified, user-asserted attributes), and elevate the contextual trust of a transaction using additional authentication methods for high risk or sensitive transactions.
- Current IDP and RP business practices may not always conform to privacy preserving practices (e.g., FIPPs data minimization), and can be managed using an AXN. A rigorous Privacy Evaluation Methodology (PEM) implementation can drive AXN technical and architectural enhancements. If implemented properly, privacy protective enhancements can greatly enhance core messaging in AX Trust Framework marketing strategy, and drive user adoption, trust and transaction volumes while enhancing RP brands.

Conclusions

This document is a work in progress. As business requirements, legal constructs, technology and protocols, and privacy policy evolve, AXN implementation requirements, data flows and technical capabilities are expected to change. Consideration should be given for these impacts and to future versions of the AX Trust Framework specification that include support for SAML, IMI, device IDs, biometrics and contextual authentication services. The AX Trust Framework contractual components are expected to simplify greatly as the AXN business models are better understood and are generally adopted by market participants.

Enterprise requirements for credential federation (using verified user-asserted attributes), attribute based access control solutions (ABAC), user managed access (UMA) solutions, and user preference management are driving innovative applications to lower costs, enable competitive differentiation, and drive new sources of revenues. Some will require user attributes to be verified by authoritative enterprise AP sources (e.g., LDAP directories or HR systems) in addition to commercial AP services for user PII. Each service will depend on the ability to bind a user to a credential used in a transaction using user-asserted, verified attributes, potentially in the context of an AX Trust Framework.

An expectation exists for several AXN's to rollout in pursuit of the credential federation and attribute exchange market and that actual implementation may vary significantly as driven by COI requirements. At the same time, AXN architecture is transaction infrastructure, or "plumbing", that will support seamless user interoperability (federated SSO with one or more credentials using verified attributes) across multiple AX Trust Framework COI implementations. The key is to get started with solutions that address market requirements so that the lessons learned will drive practical improvements while balancing the need for profitable business models that perpetuate the demand for auditable, privacy preserving, secure and user friendly applications.

Appendix A: Definitions

This Specification uses the following terms. It is important to note that the following definitions are general in nature and are provided solely to assist the reader with understanding of the foregoing text.

Attribute. A specific category of identifying information about a Subject, such as name, address, age, gender, title, salary, health, net worth, driver's license number, Social Security number, etc. (for a human being), make and model, serial number, location, capacity, etc. (for a device), etc. Synonyms: Identity Attribute

Attribute Provider (AP). A third party trusted as an authoritative source of information and responsible for the processes associated with establishing and maintaining identity attributes. An Attribute Provider asserts trusted, validated attribute claims in response to attribute requests from Identity Providers and Relying Parties. Examples of Attribute Providers include a government title registry, a national credit bureau, or a commercial marketing database.

Attribute Verification. The process of confirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information. This includes independent, standards-based processes by which user-asserted attribute claims are verified by third party sources of attribute data and/or generally accepted methods of directly verifying user attributes.

Authentication. The process of establishing or confirming that someone is who they claim to be. The process by which a person verifies or confirms their association with an electronic credential. For example, entering a password that is associated with a UserID or account name is assumed to verify that the user is the person to whom the UserID was issued. Likewise, comparing a person presenting a driver's license to the picture appearing on the license verifies or confirms that he/she is the person described in the license.

When a person presents an identity credential (such as by presenting a driver's license at an airport or entering a User ID on a corporate computer network), claims to be the User identified by the credential, and seeks to exercise a right or privilege granted to such User (e.g., to board a plane, to access the corporate network or a sensitive database), an ***authentication*** process is used by a ***Relying Party*** to determine whether that person is, in fact, who they claim to be. In other words, once someone makes a declaration of who they are (by claiming to be the person identified in the identity credential), authentication is designed to answer the question "OK, how can you prove it?" It is a transaction-specific event that involves associating a person with an identity credential to verify that the person trying to engage in the transaction really is the person that was previously identified by the credential.

Authentication typically requires something to tie the person to the credential, generally referred to as an authenticator. If the credential is a driver's license or passport, the authenticator is the picture and the association is typically done by comparing the picture on the license or passport to the person presenting it. With electronic credentials, the authenticator is typically something the User "knows" (e.g., a secret password, or personal identification number (PIN)), something the User "possesses" (e.g., a private cryptographic key, a physical device such as a smart card, USB plug-in, or other type of physical token), or something the User "is," such as a physical characteristic (e.g., a picture, fingerprint, or other biometric data).

Authenticator. Something that is used to determine authenticity; usually an object, an item of knowledge, or some characteristic of its possessor that is used to tie a person to an identity credential (such as by demonstrating that such person has possession of the authenticator). For example, a password functions as an authenticator for a UserID, a picture functions as an authenticator for a passport or driver's license.

Authoritative Party. An organization or User that is trusted to be an authority on the identity related attributes or roles associated with users and subjects of services.

Authorization. A process of granting rights and privileges to authenticated Subjects based on criteria determined by the Relying Party; designed to control access to information or resources so that only those specifically permitted to use such resources are granted access to them.

Once a person is successfully authenticated by the Relying Party, the Relying Party may use its own authorization process to determine what rights and privileges are accorded to such person – e.g., whether such person should be granted access to a website, a database, a bar, or an airport boarding area. This process addresses the question "What can you do?" In other words, authentication of identity is not just an end in itself, but rather a process used to authorize some type of grant of rights or privileges (e.g., to access and use certain system resources in the online context), to facilitate a transaction or decision, or to satisfy an evidentiary obligation. For example, once the identity of someone seeking to access to a computer system, network, or database has been authenticated, the database owner (i.e., the Relying Party) may use an authorization process to determine what access rights should be granted to the person seeking access. Likewise, once the identity of someone seeking to enter into an electronic transaction (e.g., an electronic contract) has been authenticated, a Relying Party may use an authorization process to determine whether to proceed with a transaction with the Subject or otherwise rely on the communication.

AXN Identifier. The name for the AXN listed within a given Identity Provider's Trusted AXN List. The AXN Identifier is assigned by the Identity Provider, and a given AXN may have a different identifier at each Identity Provider.

Client. A software program capable of making direct calls to API Endpoints without the use of a browser.

Consent. The process whereby an end user completes some measurable action which indicates that they understand and authorize the request being made

Context. An environment with defined boundary conditions in which entities exist and interact.

Credential. A set of data presented as evidence of a claimed identity and/or entitlements. This could take the form of a paper or digital document that authoritatively binds identity attributes about a Subject to an authenticator possessed and controlled by the Subject. This includes data used to establish the claimed attributes or identity of a person or an entity. Examples of paper credentials include passports, birth certificates, driver's licenses, and employee identity cards. Examples of digital credentials include usernames, smart cards, and digital certificates.

Digital identity A digital representation of the information known about a specific User, group or organization.

Federated Identity. The technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization. A federated identity system allows the sharing of identity credentials issued, and identity information asserted, by one or more Identity Providers with multiple Relying Parties.

Identification. The process of collecting, verifying, and validating sufficient attribute information about a specific person, legal entity, device, or digital object to define and confirm its identity within a specific context. Synonyms: Enrolment; Identity Proofing.

Identification Process is designed to answer the question "who are you?" Performed by someone filling the role of an ***Identity Provider*** it involves associating one or more identifying attributes (such as name, membership number, email, address, birth date, employer, or job title) with a person in order to identify and define that User to the level sufficient for the contemplated purpose. Sometimes called "identity proofing" or "enrolment," this process is often a one-time event. It typically involves the collection by an Identity Provider of information about the person to be identified (referred to as the "Subject"), and often relies on a patchwork of government-issued documents (e.g., a birth certificate, Social Security card, driver's license, and passport), as well as credentials issued by private sector entities (e.g., an employee badge, mobile wireless SIM card, and credit cards). Although such identity documents and credentials were issued for other purposes, they can often be re-used to facilitate later identification processes in new contexts. This occurs, for example, when someone provides a driver's license to prove their identity in the context of receiving an employee identity badge.

At the end of the identification process in the digital context, the Subject's relevant identity attributes are typically represented by data in an electronic document issued by the Identity Provider and referred to as an identity credential (e.g, an OpenID). A credential presents (or links to or correlates with) data that is used to authenticate the claimed digital identity or attributes of a person, entity, or device. A credential can be embodied in a variety of media. In the physical world, examples of an identity credential include a royal seal, a driver's license, a passport, a library card, or an employee identification badge. In the online world the identity credential might be as simple as a User ID or OpenID, or as complex as a cryptographically based digital certificate that might be stored on a computer, cell phone, smart card, ATM card, flash drive or similar device.

Identity. Information about a person, legal entity, device, or digital object in the form of one or more attributes that allow the person, legal entity, device, or digital object to be sufficiently distinguished within a particular context. The set of the attributes of a person which allows the person to be distinguished from other persons within a particular context.

For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts. In general, each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.

Identity Assurance. The degree of confidence in the process of identity validation and verification used to establish the identity of the entity to which the credential was issued, and the degree of confidence that the entity that uses the credential is that entity or the entity to which the credential was issued or assigned.

Identity Attribute. Information bound to a subject identity that specifies a characteristic of the subject.

Identity Context. The environment or circumstances in which identity information is communicated and perceived. Users operate in multiple identity contexts (e.g., legal, social, employment, business, pseudononymous) and may identify themselves differently based on the context.

Identity Management. A set of functions and capabilities (e.g., technical systems, rules, and procedures, administration, maintenance, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for the collection, verification, binding, and communication of identity information about a Subject to a Relying Party. The primary goal of identity management is to establish a trustworthy process for assigning identity attributes to a digital identity and to connect that identity to an User, legal entity, device, or digital object. Identity management includes the processes for maintaining and protecting the identity information (e.g., identifiers, credentials, attributes) of an User over its lifecycle; and, assurance of the identity of an entity and supporting business and security applications.

Identity Proofing. The verification and validation of information when enrolling new entities into identity systems through a process which validates and verifies sufficient information to confirm the claimed identity of the entity.

Identity Provider (IDP). Within a given identity system, an entity responsible for the identification of persons, legal entities, devices, and/or digital objects, the issuance of corresponding identity credentials, and the maintenance and management of such identity information for Subjects. Synonyms: Credential Service Provider (CSP); Certification Authority (CA); Attribute Provider (where single or limited attribute data is provided).

Identity System. An online environment for identity management governed by a set of operating rules where Users, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities.

Locator. An opaque string passed to the Relying Party by the AXN that is used to by the RP to access the Verified Attribute API. The Locator may be a permanent reusable identifier or may be an ephemeral context-dependent key.

Operating Rules. The specifications, rules, requirements, and obligations that govern the day-to-day operation of a specific identity system. Operating rules consist of business & technical operational rules and contractually-defined legal rules. The operating rules are typically privately developed (e.g., by the operator of the identity system), and

made binding and enforceable on the participants via contract. Synonyms: Trust Framework; System Rules; Common Operating Rules; Operating Regulations.

Pairwise Pseudonymous Identifiers (PPID). A one-way subject identifier created by the Identity Provider that differs depending on the recipient of the identifier.

Personally Identifiable Information (PII). Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an User person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

Relying Party (RP). An entity that has a need to authenticate the identity of the Subject, and that relies on an Identity Provider for identity and authentication of the Subject, typically to process a transaction or grant access to information or a system. The person or legal entity that is relying on an identity credential or assertion of identity to make a decision as to what action to take in a given application context. Synonym: **Service Provider**.

Subject. The person, legal entity, device, or digital object that is identified in a particular credential and that can be authenticated and vouched for by an Identity Provider. Synonyms include Data Subject and **User**.

Subject Identifier. A globally unique identifier created by the Identity Provider, which can be mapped to a single user account.

Trust. The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.

Trust Framework. A set of verifiable [and enforceable?] commitments from each of the various parties in a transaction to their counter parties. These commitments necessarily include(1) Controls (including regulatory and contractual obligations) to help ensure commitments are delivered and (2) Remedies for failure to meet such commitments. A trust framework is developed by a community whose members have similar goals and perspectives. It defines the rights and responsibilities of that community's participants in the Identity Ecosystem; specifies the policies and standards specific to the community; and defines the community-specific processes and procedures that provide assurance. A trust framework considers the level of risk associated with the transaction types of its participants; for example, for regulated industries, it could incorporate the requirements particular to that industry. Different trust frameworks can exist within the Identity Ecosystem, and sets of participants can tailor trust frameworks to meet their particular needs. In order to be a part of the Identity Ecosystem, all trust frameworks must still meet the baseline standards established by the Identity Ecosystem Framework.

Trust Framework Provider (TFP). An organization that translates the requirements of policymakers into its own blueprint for a trust framework that it then proceeds to build, doing so in a way that is consistent with the minimum requirements set out in this Specification.

Trust Level. A consistent, quantifiable measure of reliance on the character, ability, strength, or truth of someone or something.

User Agent. A software program capable of receiving and processing HTTPS protocol requests, such as redirections that convey header information to and from other parties. The most common user agent is a browser.

Verified Attribute. An attribute whose veracity has been confirmed by an Attribute Provider

Valentine Token. A token that is created by the Identity Provider on behalf of a Subject. The token is given to a relying party that is trusted by the subject, and can be validated only by a specific AXN that is trusted both by the subject and by the relying party. The valentine token is submitted by the AXN to the Identity Provider for validation.

Appendix B: Privacy Principle Comparison Matrix

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
The User Control Principle *[Identity assurance activities can only take place if I consent or approve them]* An Identity Assurance Provider or Service Provider must ensure any collection, use or disclosure of IA data in, or from, an Identity Assurance Service is approved by each particular Service-User who is connected with the IA data. Identity Assurance Providers or Service Providers cannot use or disclose IA data without the Service-User's knowledge and agreement (i.e. consent) Service-Users must be able to control/choose whether or not to use or disclose their IA data and whether or how they assert their identities. Any exemption from the User Control Principle should be specified via the Exceptional Circumstances Principle.	**User Control** Consumers have a right to exercise control over what personal data companies collect from them and how they use it. Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they	**Use Limitation Principle.** Personal data should not be disclosed . . . except "with the consent of the data subject or by the authority of law." **Purpose Specification Principle** 9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. **User Participation**	**Opt-in** Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of User attributes for each transaction. The goal is for the user is to understand the opt-in process, and to have a meaningful opportunity to agree. There are various ways to implement this	*Article 6* ***Lawfulness of processing*** 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; *Article 7* ***Conditions for consent*** 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal	DND: The basic concept of "user control" is the same in all of these approaches. The "opt in", rather than "opt out" is expressed in all of these documents --- either using the specific words "opt in" or conceptually. I recommend that we adopt the "opt in" approach specifically. I also would like to suggest that we add specific "Do not track" language to the template. That concept is found in the FICAM TFPAP and in the EU Proposed General Data Regulation. "DNT" is a key aspect of user trust.

[4] Source document is the FICAM Privacy Guidance for Trust Framework Assessors and Auditors

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
	collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place.	**Principle** 13. An User should have the right: • a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; • b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a	goal. Users need to be able to see each piece of information, or attribute that is to be transmitted prior to it being transmitted. The confirmation mechanism must enable the user to make an explicit affirmation to permit the transmission of user information in accordance with the notice as described above. Confirmation mechanisms should be designed so that they are intuitive and easy to use. They need to be specific to the transaction. To the extent the information to be transmitted is not required for authentication (i.e., the Relying Party would like to have the information to pre-populate transaction fields or for	data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
		reasonable manner; and in a form that is readily intelligible to him; • c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.	other reasons, but the information is not necessary to accomplish the authentication of the user), users should have the ability to expressly permit or deny the transmission of specific pieces of such user information, for example, through radio buttons or similar mechanisms. As described above, the design of the notice and the confirmation mechanism should be considered as an integrated concept. Mechanisms that allow users to affirmatively waive notices and opt-in consents for each transmission such as a "don't show me this message again" option are acceptable. Mechanisms such as a simple "agree" button on		

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
			'general terms of service' or pre-checked consents are strongly discouraged because they are unlikely to meet the essential objective of meaningful understanding. Generally, it is less meaningful to obtain opt-in at the time the credential is issued rather than at the time of the transaction. In certain circumstances, the TFET may approve TFPs that accept this practice. Assessors should be made aware of agreements made between the TFP and TFET that affirmatively accept this practice and any constraints established for this practice.		
The Transparency Principle [Identity assurance can only take place in ways I understand and when I am fully informed]	**Transparency** Consumers have a right to easily understandable and accessible	**Openness Principle.** There should be a general policy of openness about developments,	**Adequate Notice** Identity Provider must provide End Users with adequate	***Article 5 Principles relating to personal data processing*** Personal data must be:	DND: The narratives are different but the concepts of having full and transparent information

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
Each Identity Assurance Provider or Service Provider must be able to justify to Service-Users why their IA data are processed. Each Service-User, prior to using an Identity Assurance Provider or a Service Provider for the first time, must be provided with a clear description about the processing of IA data in advance of any processing. The information provided includes a clear explanation of why any specific information has to be provided by the Service-User (e.g., in order that a particular level of identity assurance can be obtained) and identifies any obligation on the part of the Service-User (e.g., in relation to the User's role in securing his/her own identity information). Any subsequent and significant change to the processing arrangements that have been previously described to a Service-User needs the prior consent or approval of that Service-User before it comes into effect. Organisations should engender trust by being open about all aspects of the processing of **IA data** (Processing means "collecting, using, disclosing, retaining, transmitting, copying, comparing, corroborating, aggregating, accessing" and anything else)**.** Such information does not need to be provided at every transaction, if the Service-User has been previously	information about privacy and security practices. At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise User Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.	practices and policies with respect to personal data. **Use Limitation Principle** 10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: • a) with the consent of the data subject; or • b) by the authority of law. Paragraph 12: Openness Principle 57. The Openness Principle may be viewed as a prerequisite for the User Participation Principle (Paragraph 13); for the latter principle to be effective, it must	notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process. Adequate notice is a practical message that is designed to help the average user understand how to engage in the authentication transaction, including, what information is being transmitted about the user, what options the user has with respect to the transmission of	(a) processed lawfully, fairly and in a transparent manner in relation to the data subject; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data; (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	provided to users are the same. We will be able to adapt the narrative and can explain to others that these core ideas are advocated by others besides the U.S.

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
informed. We expect that a public document explaining how these Principles have been applied to an **Identity Assurance Service** will be a valuable aid in meeting the objectives of this Principle (see **also** the *Governance/Certification Principle* below). Where changes occur, any Provider would have to anticipate the fact that consent or approval might not be forthcoming. Any exemption from the Transparency Principle should be specified via the Exceptional Circumstances Principle.		be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost. Paragraph 9: Purpose Specification	the information, and the consequences of refusing any transmission. For example, if the information to be transmitted is required by the Relying Party for the authentication, the notice should make clear that the transmission is required and refusal will cancel the transaction and return the user to the Relying Party's website for further assistance. If the information to be transmitted is not required for authentication, but, for example, will be collected by the Relying Party in order to provide the service requested by the user more conveniently, the notice should make this distinction clear and indicate that if the user refuses the	(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage; (f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation. *Article 11* ***Transparent information and communication*** 1. The controller shall have	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
		Principle 54. The Purpose Specification Principle is closely associated with the two surrounding principles, i.e. the Data Quality Principle and the Use Limitation Principle. Basically, Paragraph 9 implies that before, and in any case not later than at the time data collection it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, e.g., by public declarations, information to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies.	transmission, the user will be able to provide the information directly on the Relying Party's website. Assessors and Auditors should look for a notice that is generated at the time of the authentication transaction. The notice should be in visual proximity (i.e. unavoidable) to the action being requested, and the page should be designed in such a way that any other elements on the page do not distract the user from the notice. The content of the notice should be tailored to the specific transaction. The notice may be divided into multiple or "layered" notices if such division makes the content more understandabl e or enables users to make more	transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child. *Article 14* ***Information to the data subject*** 1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
		According to Paragraphs 9 and 10, new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like. Paragraph 10: Use Limitation Principle 55. This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified	meaningful decisions. For these reasons, the notice should be incorporated into the "opt in" mechanism as set forth below. In sum, an Adequate Notice is never just a link somewhere on a page that leads to a complex, legalistic privacy policy or general terms and conditions. **No activity tracking** Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002. The purpose of this principle is	and of the data protection officer; (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (c) the period for which the personal data will be stored; (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data; (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (f) the recipients or categories of	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
		purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative - see Paragraph 52 above) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and	to ensure that the Identity Provider does not use or disclose any information about the user and his or her interactions with the government, which the Identity Provider learns as a result of providing the authentication service for any purpose other than to provide the authentication service. Assessors and Auditors should check for a written policy that demonstrates how the Identity Provider will comply with this principle. Assessors and Auditors should also evaluate the effectiveness of the means, technical or otherwise, which the Identity Provider uses to achieve compliance. Finally, Assessors and Auditors	recipients of the personal data; (g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission; (h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected. 2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
		social planning.	should check whether the Identity Provider provides an explanation of this principle to users. This explanation may be located in a general privacy policy about the collection and use of personal information.	possible consequences of failure to provide such data.	
The Multiplicity Principle *[I can use and choose as many different identifiers or identity providers as I want to]* A **Service-User** is free to use any number of identifiers that each uniquely identifies the individual or business concerned. A **Service-User** can use any of his identities established with an **Identity Assurance Provider** with any **Service Provider**. A **Service-User** can choose any number of **Identity Assurance Providers** or **Service Providers** in order to meet his or her diverse needs. A **Service-User** shall not be obliged to use any **Identity Assurance Provider** or **Service Provider** not chosen by that **Service-User; however, a Service Provider** can require the **Service-User** to provide a specific level of Identity Assurance, appropriate to the **Service-User's** request to a					I agree with Rich's points. This is an especially tough issue to tackle without knowing more about how users will learn about, and have access to, SPs. DBR- if you look at the swimlanes it appears this maybe the responsibility of the AXN as that is where the User Admin Console attributes and sharing

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
Service Provider. A **Service-User** can terminate, suspend or change **Identity Assurance Providers** or **Service Providers** at any time A Service Provider does not know the identity of the Identity Assurance Provider used by a Service-User to verify an identity in relation to a specific service These first three need no explanation. Where Service Providers are a monopoly or near monopoly, they should not be able to require a particular Identity Assurance Provider to be used. However, a Service Provider must be able to insist on a particular (and not unreasonable) level of identity assurance before delivering a service. Any exemption from the Multiplicity Principle should be specified via the use of the Exceptional Circumstances Principle. It should not be possible to link a Service-User's activities in different contexts.					with relying parties will be controlled by the user.
The Data Minimisation Principle *[My request or transaction only uses the minimum data that is necessary to meet my needs*] **IA data processed** by an **Identity Assurance Provider** or a **Service Provider** to facilitate a request of a **Service-User** must be the minimum necessary in order	**Focused Collection** Consumers have a right to reasonable limits on the personal data that companies collect and retain. Companies should collect	**Collection Limitation Principle.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate,	**Minimalism** Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile.	*Article 5* ***Principles relating to personal data processing*** Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
to fulfil that request in secure and auditable manner. END PRINCIPLE ***Note**: it is useful to remind the reader that this Principle has a wide reach because of the definitions of **IA data** and **Processing:*** • ***"IA data** includes "Personal data", "Audit data, "Attribute data, "Identity data", "Relationship data"; "Transactional data" and other "General data"* ***"Processing"** in the context of IA data means "collecting, using, disclosing, retaining, transmitting, copying, comparing, corroborating, aggregating, accessing"... etc***).** So for the absence of doubt, any aggregation, correlation or corroboration of IA data from diverse Identity Assurance Providers or Service Providers are subject to all the Identity Assurance Principles. All IA data processed has to be the minimum necessary in the context of service delivery or identity verification. Note that a Service User can, for his own convenience, request a Provider to hold information beyond the minimum necessary. Subject to any audit or legal requirement, the Minimisation Principle	only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise. **Respect for Context** Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with	with the knowledge or consent of the data subject.	RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002. Assessors and Auditors need to ensure that Identity Providers are only sending the information that is explicitly requested by the Relying Party or that is required by the Federal profile. Written documentation is important in ensuring that the Adequate Notice and Opt-in principles are appropriately executed in terms of distinguishing between information that the Relying Party needs to conduct the authentication transaction and information that the	data subject; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
requires any aggregation, correlation or corroboration to be of a transient nature. Data minimisation is a very important design criterion; we expect compliance with this Principle will be an essential component of any **Identity Assurance Service**. Any decision that requires a risk assessment of the Service-User will need the correlation of data from possibly a number of sources will also be subject to the Data Minimisation Principle Note that the User Control or Transparency Principle should ensure the Service-User can provide informed consent/approval. There should be no centralisation of IA data. Any exemption from the Data Minimisation Principle should be specified via the Exceptional Circumstances Principle.	consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Control by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and		Relying Party would like to collect. In the absence of any such written documentation from the Relying Party, only the information required by the Federal profile may be sent.		

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
	familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults.				
The Data Quality Principle *[I choose when to update my records]* **Service-Users** should be able to update their own **personal data**, at a time at their choosing, free of charge, and in a simple and easy manner. **Identity Assurance Providers** and **Service Providers** must take account of the appropriate level of identity assurance required before allowing any updating of **personal data**.	**Access and Accuracy** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if	**Data Quality Principle** 8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.		*Article 15* ***Right of access for the data subject*** 1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
Unnecessary retention and excessive data collection would breach of the *Data Minimisation Principle.* If a Service User fails to keep his information up to date, then his transactions could fail; this we believe is the incentive for Users to keep information up to date. Any legal obligation that requires, for example, an individual to notify a public authority of a change of circumstances is unaffected; a Service-User can choose to use an Identity Assurance System, at any chosen time, to update their own records subject to any identity assurance requirement prior to accepting an update. As failed transactions (e.g., by virtue of a data mismatch) are likely to be alerted to Service-Users, this affords a possibility of designing procedures that offer Service-Users the opportunity to update their own details immediately – again subject to any identity assurance requirement prior to accepting any update. The Identity Assurance/Service Provider has to be able to decide the level of identity assurance before accepting a change to a Service User's data. Any exemption from the Data Quality Principle should be specified via the Exceptional Circumstances Principle.	the data is inaccurate. Companies should use reasonable measures to ensure they maintain accurate personal data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures they may use to maintain accuracy and to provide access,	Paragraph 8: Data Quality Principle 53. Requirements that data be relevant can be viewed in different ways. In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection. The conclusion of the Group was to the effect, however, that data should be related to the purpose for which they are to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation, and the same is true of evaluative data. Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept. The		being processed, the controller shall provide the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries; (d) the period for which the personal data will be stored; (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (g) communication of the personal data undergoing processing and of any	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
	correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm.	requirements in this respect are linked to the purposes of data, i.e. they are not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of archives. The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.		available information as to their source; (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20. 2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject. *Article 16* ***Right to rectification*** The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
				incomplete personal data, including by way of supplementing a corrective statement. *Article 17* ***Right to be forgotten and to erasure*** 1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
				when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons.	
The Service-User Access and Portability Principle *[I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want]* Each **Identity Assurance Provider** or **Service Provider** must allow, promptly, on request and free of charge, each **Service-User** access to any **IA data** that relates to that **Service-User**. It shall be unlawful to make it a condition of doing anything in relation to a **Service-User** to request or require that **Service-User** to request **IA data.** The **Service-User** shall have the right to require an **Identity Assurance Provider** to transmit his **personal data,** to a second **Identity**	**Accountability** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights. Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for	Paragraph 14: Accountability Principle 62. The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly. it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation		***to data portability*** 1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject. 2. Where the data subject has provided the personal data and the processing is	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
Assurance Provider in a standard electronic format, free of charge and without impediment or delay. The Service-User's right to data portability shall also apply between Service Providers. For the absence of doubt, such access includes access to logs of Service-User activity, disclosure logs of any Service-User data, and any audit data relating to that Service-User's activity but excludes any anonymised data that can no longer be linked or associated with a particular Service-User. The prohibition is needed as there is a practice in the UK of requiring data subjects to use their subject access rights to criminal records and medical records and show the product of their access request to an employer or insurer. The prohibition stops unscrupulous use of the access right. The text is based on the prohibition in the ID Card Act 2005. This is the right to data portability. Any exemption from the Service-User Access and Portability Principle should be specified via the Exceptional Circumstances Principle.	adhering to these principles. To achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise.	merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance. Paragraph 13: Individual Participation		based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
		Principle 58. The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language. With respect to the individual sub-paragraphs, the following explanations are called for. 59. The right to access should as a rule be simple to exercise. This may mean, among other things, that it should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or			

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
		similar measures. In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical area a medical practitioner can serve as a go-between. In some countries supervisory organs, such as data inspection authorities, may provide similar services. The requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests. Normally, the time is to be counted from the receipt of a request. Its length may vary to some extent from one situation to another			

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
		depending on circumstances such as the nature of the data processing activity. Communication of such data "in a reasonable manner" means, among other things, that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable. The extent to which data subjects should be able to obtain copies of data relating to them is a matter of implementation which must be left to the decision of each Member country.			
The Governance/Certification Principle *[I can have confidence in any Identity Assurance System because all the participants have to be accredited]* As a baseline control, all **Identity Assurance Providers**	**Security** Consumers have a right to secure and responsible handling of personal data. Companies	**Security Safeguards Principle** 11. Personal data should be protected by reasonable security	**Termination** In the event an Identity Provider ceases to provide this service, the Provider shall continue to	*Article 22* ***Responsibility of the controller*** 1. The controller shall adopt policies and implement appropriate measures to ensure and be	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
and **Service Providers** shall be certified. There shall be a certification procedure subject to an effective independent audit regime which ensures that all relevant, recognised identity assurance and technical standards, data protection or other legal requirements are maintained by **Identity Assurance Providers** and **Service Providers.** In the context of **personal data**, certification procedures include the use of Privacy Impact Assessments and Privacy by Design concepts. All **Identity Assurance Providers** and **Service Providers** shall take all reasonable steps to ensure that a **Third Party** cannot capture **IA data** that confirms (or infers) the existence of relationship between any **Participant.** Certification can be revoked if there is significant non-compliance with any **Identity Assurance Principle**. The architecture of an Identity Assurance Service must be based on open standards. This Principle mandates the use of all relevant standards as the baseline for all information assurance/security/integrity controls used. We expect that this Principle will require the production of document that describes how the design of the **Identity Assurance Service** has been informed by the application of the Identity Assurance	should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure. **Accountability** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights. Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for adhering to these principles. To	safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. **Accountability Principle** 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.	protect any sensitive data including PII. Assessors and Auditors should evaluate whether the written policy or plan expressly provides for destruction of the data, as appropriate, or a commitment that the Identity Provider, to the best of its abilities, will require that any recipient of the data protect the data in kind. Ideally, Identity Providers also should plan to give users notice when their sensitive data will be transferred to another entity.	able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1). 3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
Principles to the design (See also the *Transparency Principle* above). The "reasonable steps" tries to ensure that web-based services (Google; Facebook and perhaps more unscrupulous browsers) cannot capture details of a relationship between **Service Users** and any **Identity Assurance Provider** or **Service Provider** used by them even though the **Service-User** might have unwittingly allowed it. (Note: this is why **relationship data** includes in its definition relevant cookies and programs that collect such data). Any exemption can be specified via use of the Exceptional Circumstances Principle, but we don't expect many (or indeed any!). The Accountability Principle in the Data Protection Regulation (currently under discussion in Europe); the current obligations in the Seventh Data Protection Principle (or HMG Security Framework or ISO27000) are expected to form part of the Certification process. Privacy Impact Assessments and Privacy by Design concepts will be legal obligation if the European Commission's Data Protection Regulation becomes law (see under the heading Data Protection by Design and Data Protection Impact Assessments) Consideration needs to be given as to whether it should be made unlawful for such details to be captured (even overriding any User's explicit	achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise.			2. If proportionate, this verification shall be carried out by independent internal or external auditors. *Article 23* ***Data protection by design and by default*** 1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. 2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
consent). We are ***very*** concerned that many Users do not know what permissions they have given nor do they read privacy policies of organisations based outside the EEA. **There is a need to take away the defence of a Third Party that it has the permission of the User to capture details from an Identity Assurance Service.**				processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals. *Article 30* ***Security of processing*** 1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. 2. The controller and the processor shall, following an evaluation of the risks, take the	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
				measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data. *Article 32* ***Communication of a personal data breach to the data subject*** 1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
				shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3). 3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. *Article 39* ***Certification*** The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks,	

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
				allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.	
The Problem Resolution Principle *[If there is a problem I know there is an independent arbiter who can find a solution]* A **Service-User**, who after a reasonable time, cannot or is unable to resolve a complaint or problem directly with a **Identity Assurance Provider or Service Provider** can call upon an independent Identity Ombudsman to seek independent resolution of the issue. As part of the certification process**, Identity Assurance Providers** and **Services Providers** are obliged: i. (a) to co-operate with the Identity Ombudsman and accept his impartial determination and, i. (b) to ensure that	**5. ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.** Companies should use reasonable measures to ensure they maintain accurate personal data. Companies				

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
contractual arrangements • (i) reinforce the application of the **Identity Assurance Principles**, and • (ii) contain a reference to the Identity Ombudsman as a mechanism for problem resolution. The Identity Ombudsman can resolve the same or similar complaints affecting a group of **Service-Users.** The Identity Ombudsman can co-operate with other Regulators in order to resolve problems and can raise relevant issues of importance concerning an **Identity Assurance Service.** An adjudication/recommendation of the Identity Ombudsman shall be published. There can be more than one Identity Ombudsman. The Identity Ombudsman can recommend changes to standards or certification procedures or that an Identity Assurance Provider or Service Provider should lose their certification. The central problem is that many different Regulators (e.g., Information Commissioner; FSA, OFCOM) could be involved and that an individual has to be able to complain to a central point of contact in order to resolve an issue. Without an Ombudsman/Advocate, there	also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures they may use to maintain accuracy and to provide access, , deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they				

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
is a risk that the Service User will be passed from pillar to post. One assumes, however, that a Service-User will resolve a complaint in the usual way. However, it is possible that complaints will not be resolved satisfactorily. We expect that any determination made by an Identity Ombudsman can be appealed to the Courts by any party to the dispute. Any exemption from the Problem Resolution Principle can be specified via use of the Exceptional Circumstances Principle (**but we can't see the need of any exemption as explained as follows).** Take an extreme example, and suppose there was an exemption needed for say "national security", then the Regulator who has the responsibility for the national security function could be designated as the "ombudsman" for that purpose. This would maintain the integrity of this Principle and the secrecy required of the national security function.	collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm.				
The Exceptional Circumstances Principle *[Any exception has to be approved by Parliament and is subject to independent scrutiny*] Any exemption from the application of any of the above Principles to **IA data** shall **only** be lawful if it is specified in the statutory framework established by the					

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
general legislation needed to legitimise all **Identity Assurance Services**. Any exemption from the application of any of the above Principles that relates to the **processing** of **personal data** must also be necessary and justifiable in terms of one of the criteria in Article 8(2) of the European Convention of Human Rights: namely in the interests of national security; public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals, or for the protection of the rights and freedoms of others. Any subsequent **processing** of **personal data** by any **Third Party** who has obtained such data in exceptional circumstances (as identified by Article 8(2) above) must be the minimum necessary to achieve that (or another) exceptional circumstance. Any exceptional circumstance involving the **processing** of **personal data** must be subject to a Privacy Impact Assessment by all relevant "data controllers" (where "data controller" takes its meaning from the Data Protection Act). Any exemption from the application of any of the above Principles in relation to IA data shall remain subject to *The Problem Resolution Principle*. There a myriad of data sharing laws each with different standards and rules. To engender trust in the					

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
identity assurance and to improve Parliamentary scrutiny, it is proposed that **ONLY** statutory gateways created by the legislation needed to establish the programme are valid. There might be a phasing in period (as discussed in the workshop). The special interests identified in Article 8(2) are expressly put into this Principle. However, the linkage to individual human rights means that the link can only relate **to personal data** (i.e. an identifiable living individual)**.** This is why a definition of "**personal data"** is needed This allows for limited onward data sharing, so long as it is consistent with Article 8 of the HRA. **There is a real issue as to whether the current level of privacy protection is adequate** for some public bodies (e.g., is the protection in RIPA adequate? is the Regulatory regime for the Security Service, GCHQ or the Police OK?). Our construction avoids the opening up what would be an everlasting debate; however, the last paragraph of this Principle is the necessary "*quid pro quo*" for this position. (See comments at the bottom of Principle 8 re Governance on national security) We understand that legislation is under consideration to implement the Government's Identity Assurance Plans. Such legislation would be the					

The Privacy and Consumer Advisory Group to the UK Government's IDA Programme	US Consumer Privacy Bill of Rights	OECD Privacy Guidelines	US FICAM TFPAP Privacy Criteria[4]	Draft EU Data Privacy Regulation	Comments
natural vehicle to describe all "exceptional circumstances." It is expected that any exemption will be limited, and expressed in terms of particular subsets of **IA data (e.g., "personal data", "audit data", "relationship data")** necessary for the application of any exemption. The European Commission's Data Protection Regulation calls for mandatory Data Protection Impact Assessments (i.e. Privacy Impact Assessments).					

Appendix C: Use Cases

Contextualizing Risk Management Decisions Use Cases

VISION

- Policy based approach to securing online transactions & interactions
- Comprehensive risk management strategies
- Protect people's identity & data to enable a safer, more trusted connected society
- Richer set of verified attributes for better risk management decisions
- Quantify & manage risk from unmanaged devices, locations and users to protect IP
- Protect people's identity includes privacy protection

Scenario 1: BYOD Use Case 1

- Senior organization officer brings their new tablet device – they want to access corporate resources on it including email and apps
- IT wants to ensure proper controls and protections are in place appropriate to risk associated with user's network activities

Goal: Enable more secure productivity on many devices and from many locations

Agent install on the employee's device (MDM)

- Overall context
  - User choice and flexibility are increasingly important for productivity
  - Users want to use devices of their choice for both work and personal purposes
  - IT wants to ensure data and IP protection mechanisms are in place regardless of device
- Goals
  - Allow users to bring their own device and access organizational resources
  - Protect users and corporate data
  - Allow granular levels of access based on gradated trust levels
- Risks to quantify and manage
  - Unknown devices and unknown security on those devices
  - Protection of user data on their device vis-à-vis organization's data and IP
  - Strength of the initial provisioning process (user identity, in-person proofing, tying device to user)
- How Adaptive Access solves this scenario
  - Granular attributes – tying classes of attributes together for a granular access solution
  - Verified device attributes based on agent data from device to authorize the device & tie to the user
  - Distinct data stores for different types of data based on data attributes

Scenario 1: BYOD Use Case 2

- No agent install – non-MDM use case
- Overall context
  - User choice and flexibility are increasingly important for productivity
  - Users want to use devices of their choice for both work and personal purposes
  - IT wants to ensure data and IP protection mechanisms are in place regardless of device
- Goals
  - Allow users to bring their own device and access organizational resources
  - Protect users and corporate data
  - Allow granular levels of access based on gradated trust levels
- Risks to quantify and manage
  - Unknown devices and unknown security on those devices
  - Protection of user data on their device vis-à-vis organization's data and IP
  - Problem of the lying endpoint – use of network and other external sensors
  - approach: in each sub use case develop risk and mediation
- How Adaptive Access solves this scenario
  - Externally verified attributes for device for granular access (network sensors, etc.)
  - Variable access based on amount and quality of information collected about a device
  - Granular attributes – tying classes of attributes together for a granular access solution

Scenario 2: B to C: Retail Transactions

- Many different attributes needed for a transaction
- Common characteristics: person, device, network location, behaviors
- Online retail commerce (Amazon purchase)
- Online healthcare – ACA – access to data & controls – risk mediation & protection of data
  - Enabling access where needed

Scenario 2 B to C: Healthcare Use Case 1

- Overall context
  - $27 billion (HITECH) Act, to digitize the nation's medical records and rewire healthcare for the 21st century.
  - Stage 2 of the HITECH Act EHR incentive program, hospitals and doctors must provide patients the ability to access, download and transmit their health records online.
  - "We have to make sure it's the patient on the other end of the keyboard" said Farzad Mostashari, M.D., national coordinator for health IT Nov 29th, 2012
- Goals
  - Simplify patient access to online medical records
  - Secure patient access to online medical records
  - Reduce cost through automation wherever possible
- Risks to quantify and manage
  - Identity risk: Proving that the requestor is the legitimate owner of these patient records
  - Authentication risk: Proving that returning users are who they say they are
  - Contextual risk: prove that contextual factors such as location are compliant with patient details
- How Adaptive Access solves this scenario
  - Adaptive access can simplify identity proofing by anchoring a user to a Mobile number / mobile subscription and using a matching service to match name and address attributes

  - Adaptive access can provide transparent multi-factor authentication in the form of strong device identity
  - Adaptive access can be used to obtain location attributes to minimize contextual risk

Scenario 3 B2B: Secure Collaboration - ABAC

- Org A and B are collaborating on a project
- Employee from Org B needs to access resources in Org A
- Org A has controls and policy requirements but does not control or manage either the device or user credentials of Org B employees

Scenario 4: G to C Services

- eFile Tax Returns
  - Verify secure attributes including devices and user identity
  - Current situation: Millions of dollars in fraudulent online submissions
- State and local government online services
  - DOL transactions
  - Permits and approvals processes for various transactions, e.g., Agriculture permits
- Federal Credential Cloud Exchange - FICAM trust framework – federate credential with the use of verified user attributes

Scenario 5: Online access to Healthcare records

Context:

- $27 billion HITECH Act to computerize all health data by 2015.
- HIPAA Privacy and Security Rules violation maximum penalty increased to $1.5M
- Illustrative example: Cignet fined $3m for not providing 41 patients with access to their medical records

Use cases for online access to medical records:

- Identity Proofing:
  - Process for ensuring the person requesting remote access is the actual patient (or that patient's authorized representative) and provisioning access and credentials.
    - In person visit required to provision
    - Online account provisioning
- Authentication / Adaptive Access
  - Best practices for on-going access control and maintaining regulatory compliance (username & password is not enough)
- Getting to online records remotely while traveling
- RPs needs access based on various factors including location
- Another remote access scenario is for staff to access records while they are on the road
- Scenarios should address scope of access - to what and how much do they get access - scope is preference and context
- Access to emergency response personnel at an accident scene

Appendix D: Technical Implementer's Guide

Attribute Exchange Trust Framework

Technical Implementer's Guide

DRAFT Technical Specification v 1.0

Document Version: 1.0 Serial No.

Date: 2 July 2013

Terms and Conditions

This specification was developed and is being released under this open source license by Open Identity Exchange (OIX).

Use of this specification is subject to the disclaimers and limitations described below. By using this specification you (the user) agree to and accept the following terms and conditions:

1. This specification may not be modified in any way. In particular, no rights are granted to alter, transform, create derivative works from, or otherwise modify this specification. Redistribution and use of this specification, without modification, is permitted provided that the following conditions are met:

- Redistributions of this specification must retain the above copyright notice, this list of conditions, and all terms and conditions contained herein.
- Redistributions in conjunction with any product or service must reproduce the above copyright notice, this list of conditions, and all terms and conditions contained herein in the documentation and/or other materials provided with the distribution of the product or service.
- OIX's name may not be used to endorse or promote products or services derived from this specification without specific prior written permission.

2. The use of technology described in or implemented in accordance with this specification may be subject to regulatory controls under the laws and regulations of various jurisdictions. The user bears sole responsibility for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such laws or regulations.

3. THIS SPECIFICATION IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. OIXAND EACH OIX MEMBER DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, QUIET ENJOYMENT, ACCURACY, AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER OIX NOR ANY OIX MEMBER WARRANTS (A) THAT THIS SPECIFICATION IS COMPLETE OR WITHOUT ERRORS, (B) THE SUITABILITY FOR USE IN ANY JURISDICTION OF ANY PRODUCT OR SERVICE WHOSE DESIGN IS BASED IN WHOLE OR IN PART ON THIS SPECIFICATION, OR (C) THE SUITABILITY OF ANY PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF OIX OR ANY THIRD PARTY.

4. IN NO EVENT SHALL OIX OR ANY OIX MEMBER BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS SPECIFICATION, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S OR OIX MEMBER'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS SPECIFICATION, THE USER WAIVES ANY SUCH CLAIM AGAINST OIX OR ANY OIX MEMBER RELATING TO THE USE OF THIS SPECIFICATION. IN NO EVENT SHALL OIX OR ANY OIX MEMBER BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO ANY USER OF THIS SPECIFICATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. OIX reserves the right to modify or amend this specification at any time, with or without notice to the user, and in its sole discretion. The user is solely responsible for determining whether this specification has been superseded by a later version or a different specification.

6. These terms and conditions will be interpreted and governed by the laws of the State of _____ without regard to its conflict of laws rules. Any party asserting any claims related to this specification irrevocably consents to the personal jurisdiction of the U.S. District Court for the _____ and to any state court located in such district of the State of _____ and waive any objections to the venue of such courts

Document Change History

Version Number	Version Date	Information Affected	Author(s)	Authorized by
0.1	15 March 2013	Appendices B and C taken from December 12 version of Trust Framework Specification. Overall formatting and attempt to start creating semi-normative requirements	Pamela Dingle	OIX AXWG technical subcommittee
0.2	27 March 2013	Group Review	Pamela Dingle	OIX AXWG technical subcommittee
0.3	23 April 2013	Changes made as a result of group review of the document	Pamela Dingle	OIX AXWG technical subcommittee
0.4	1 May 2013	Changes to Verified Attribute API section	Pamela Dingle, Scott Rice	OIX AXWG technical subcommittee
0.5	5 June 2013	Added “authentication” sections, and created the “RP Redirection to AXN section”	Pamela Dingle	OIX AXWG technical subcommittee
0.6	10 June 2013		Pamela Dingle	OIX AXWG technical subcommittee
0.7	21 June 2013		Pamela Dingle	OIX AXWG technical subcommittee
0.8	21 June 2013	Minor Formatting Updates and typo fixes	Scott Rice	OIX AXWG technical subcommittee

TABLE OF CONTENTS

Table of Figures

Introduction

Audience

This guide is intended for technical resources requiring deep detail about interaction requirements for framework protocol participants within the OIX attribute exchange network.

Executive Summary

An attribute exchange network is a design pattern for standards-based exchange of identity information between multiple parties. While the official Trust Framework Specification details the full complement of technical, process and policy requirements necessary to form a full attribute exchange network, this guide only details the protocol interactions necessary to allow an end user to make a consent-driven connections between member parties of an Attribute Exchange Network, such that those parties might interact with each other to assert and consume identity attributes.

Each role in an Attribute Exchange Network comes with different obligations – the only obligations documented here are the protocol-level obligations. To understand all of the requirements to be a compliant trust framework participant, see the Attribute Exchange Trust Framework Specification.

Contributors

- Pamela Dingle, Ping Identity
- George Fletcher, AOL
- Chris Donovan, ID/Dataweb
- John Bradley, Ping Identity
- Scott Rice, Pacific East
- Ravi Batchu, ID Dataweb
- David Coxe, ID Dataweb

Overview

Goals

The overall goal of an attribute exchange network is to make verified attributes available to a Relying Party, with the participation and consent of the owner of those attributes (known as the subject in this document), as supervised and validated by that end user's Identity Provider. There are many ways to exchange attributes without the knowledge and consent of the user, but those methods tend to be proprietary and opaque to the user. This document attempts to describe a general pattern that can can be reliably implemented and tested.

Attribute Exchange Network Participants

The following roles are defined for interaction with AXN:

1. ***Subject:*** The subject is the human whose identity is linked to the attributes being exchanged, and who is present and operating the user agent to authenticate to the Identity Provider and consent to exchange of attribute information.
2. ***User Agent:*** Software operated by the subject that is capable of receiving and processing HTTPS protocol requests, such as redirections that convey header information to and from other parties. The most common user agent is a browser.
3. ***Relying Party (RP):*** The RP is the protocol entity wishing to consume verified attributes. Usually the consumption of verified attributes is initiated by some user action such as a request for access to services.

4. ***Identity Provider (IDP):*** The IDP is the protocol entity that collects and asserts a persistent identifier (e.g., an OpenID credential) on behalf of the user. The IDP is responsible for protecting the integrity of this identifier and all tokens, scopes, attributes and consent exist relative to that identifier.
5. ***Attribute Provider (AP):*** An AP is the protocol entity that wishing to provide verified information about a user, however, the AP does not have any direct relationship to the end user.
6. ***Attribute Exchange Network (AXN):*** The AXN is the protocol entity that acts as a transaction and claims manager, interacting with all the protocol entities to ensure that user-asserted attributes are securely verified by participating APs, attribute claims from the AP are delivered with the user-asserted attributes to the RP, all with the consent of the user and all with the context of an identity that is asserted by an IDP. The AXN also collects revenues and distributes payments on behalf of network participants in accordance with the AXN business model, and provides a user interface whereby users can manage the distribution of verified attributes. The AXN does not store user attribute information, but uses an OpenID credential as an account reference key.

High Level Steps

A succession of browser redirects and API requests are required to request access, verify consent, and communicate information between attribute exchange network parties.

User Redirections

Happy Path User Redirection

The following diagram shows browser redirections in a successful attribute exchange, in the case where the subject already knows and consents to let both the AXN and the Relying Party work with the Identity Provider to exchange attributes. Note that solid arrows represent browser redirections, while dotted lines represent server-to-server API calls, and that the final API call to the AXN Verified Attribute API is shown here even though it is not a browser-based redirection to show the final step of retrieving actual attributes.

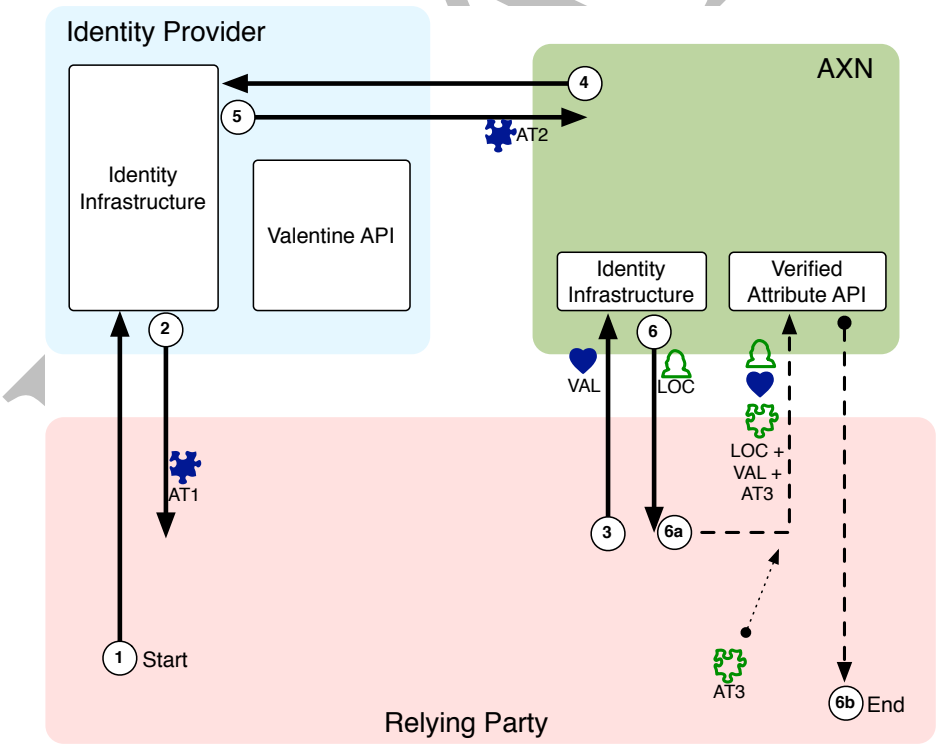


Figure 1: Happy Path Attribute Exchange with Browser Redirections

The steps shown in Figure 1, above, are as follows:

- **Identity Assertion Request**
  A request made by the Relying Party to the Identity Provider to ascertain the identity of the subject and to obtain consent for the Relying Party to interact with the Identity Provider Valentine API.
- **Identity Assertion Response**
  On successful authentication and authorization of the Relying Party, an OAuth 2.0 access token (AT1) will be returned to the Relying Party that can only be used by the Relying Party to query the trust list for the authenticated subject and to generate Valentine tokens for AXNs that are in the trust list.
- **Locator Request with Valentine token**
  The Relying Party redirects the subject's browser to the AXN, including the Valentine token.
- **Identity Assertion Request**
  A request made by the AXN to the Identity Provider to ascertain the identity of the subject and to obtain consent for the AXN to interact with the Identity Provider Valentine API.
- **Identity Assertion Response**
  On successful authentication of the subject and authorization of the AXN as a trusted client within the attribute exchange context, the Identity Provider issues to the AXN an OAuth 2.0 access token (AT2) that can only be used by the AXN to update the trust list of the authenticated subject with AXN information and to validate Valentine Tokens for the authenticated subject.
- **Successful Locator Response**
  The AXN redirects the subject's browser to the Relying Party, returning a locator to the Relying Party that can be used to access the AXN Verified Attribute API for this particular interaction.
    - **Verified Attribute API Request**
      The Relying Party uses the locator in conjunction with the Valentine token and optionally a pre-configured API access token (AT3) in a server-to-server API request to the AXN to retrieve the verified attributes.
    - **Verified Attribute API Response**
      Actual verified attributes are returned to the Relying Party.

Happy Path User Redirection with Valentine API Calls

In addition to the final server-to-server "back-channel" API calls that are documented above, additional back-channel calls are made from the Relying Party to the Identity Provider and from the AXN to the identity provider to determine whether a given AXN is trusted by the subject, and request a Valentine token representing the subject (on the part of the Relying Party) or to update the subject's trust of an AXN and validate a presented Valentine token (on the part of the AXN). The following diagram shows all of the front-channel (solid line) browser redirections and the back-channel (dotted line) API requests and responses that occur in the happy path case where the subject already trusts the AXN prior to the beginning of the flow.

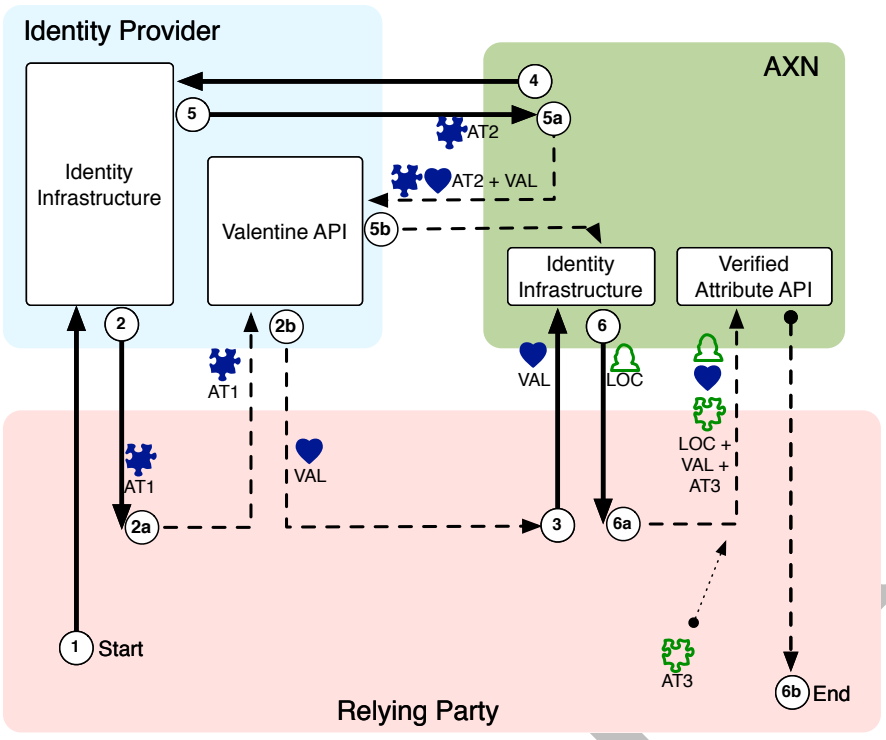


Figure 2: Happy Path Attribute Exchange with Redirects and API calls

- **Identity Assertion Request**
  A request made by the Relying Party to the Identity Provider to ascertain the identity of the subject and to obtain consent for the Relying Party to interact with the Identity Provider Valentine API.
- **Identity Assertion Response**
  On successful authentication and authorization of the Relying Party, an OAuth 2.0 access token (AT1) will be returned to the Relying Party that can only be used by the Relying Party to query the trust list for the authenticated subject and to generate Valentine tokens for AXNs that are in the trust list.
  - **Valentine API Requests**
    The Relying Party must first ascertain whether the currently authenticated subject already trusts the AXN and then must request a valentine token for the AXN (specific to the subject)
  - **Valentine API Response**
    In the case that the subject trusts the specified AXN, a valentine token will be generated for that AXN and returned to the Relying Party.
- **Locator Request with Valentine token**
  The Relying Party redirects the subject's browser to the AXN and includes the valentine token in the request.
- **Identity Assertion Request**
  A request made by the AXN to the Identity Provider to ascertain the identity of the subject and to obtain consent for the AXN to interact with the Identity Provider Valentine API.
- **Identity Assertion Response**
  On successful authentication of the subject and authorization of the AXN as a trusted client within the attribute exchange context, the Identity Provider issues to the AXN an OAuth 2.0 access token (AT2) that can only be used by the AXN to update the trust list of the authenticated subject with AXN information and to validate Valentine Tokens for the authenticated subject.
  - **Valentine API Token Validation Request**
    The AXN submits the valentine token along with the AT2 access token to the Valentine API.
  - **Valentine API Response**

The Identity Provider checks that AT2 represents the same subject as the valentine token and is targeted for the same client, the AXN. If this is true a positive validation result is returned.

- **Successful Locator Response**
  The AXN redirects the subject's browser to the Relying Party, returning a locator to the Relying Party that can be used to access the AXN Verified Attribute API for this particular interaction.
  - **Verified Attribute API Request**
  The Relying Party uses the locator in conjunction with the Valentine token and optionally a pre-configured API access token (AT3) in a server-to-server API request to the AXN to retrieve the verified attributes.
  - **Verified Attribute API Response**
  Actual verified attributes are returned to the Relying Party.

User Redirection Steps for Unknown AXN

In the case where a subject does not have a pre-existing relationship with an AXN, the Relying Party has to redirect the subject to the AXN without a valentine token to create a relationship with the Identity Provider. Then the AXN must redirect the subject back to the Relying Party to generate a valentine token.

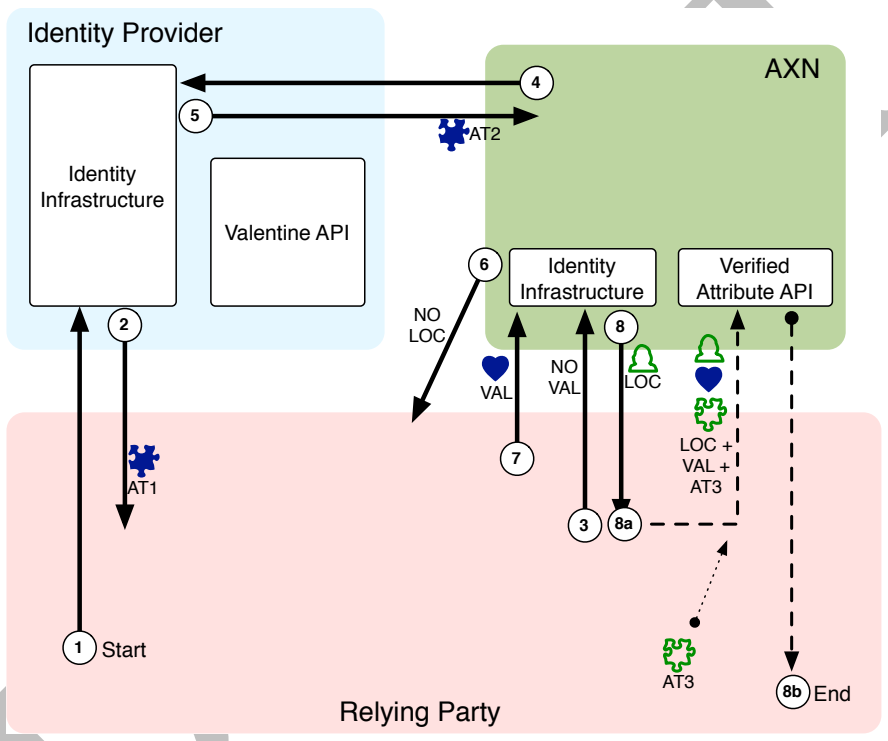


Figure 3: Unknown AXN Attribute Exchange with Browser Redirects

The steps shown in Figure 3 are as follows:

a. Identity Assertion Request
A request is made by the Relying Party to the Identity Provider to ascertain the identity of the subject and to obtain consent for the Relying Party to interact with the Identity Provider Valentine API.

b. Identity Assertion Response
On successful authentication and authorization of the Relying Party, an OAuth 2.0 access token (AT1) will be returned to the Relying Party.

c. Empty Locator Request
The Relying Party redirects the subject's browser to the AXN, but cannot include the Valentine token, because the AXN is not yet trusted by the subject.

d. Identity Assertion Request

A request is made by the AXN to the Identity Provider to obtain consent for the AXN to interact with the Identity Provider Valentine API.

e. Identity Assertion Response

On successful authentication of the subject and authorization of the AXN as a trusted client within the attribute exchange context, the Identity Provider issues to the AXN an OAuth 2.0 access token (AT2)

f. Empty Locator Response

The AXN redirects back to the Relying Party without a locator, so that the Relying Party can now fetch a Valentine token.

g. Locator Request with Valentine token

The Relying Party can now request a valentine token that is targeted to the AXN on behalf of the subject. The Relying Party again makes a Locator Request, this time including the valentine token.

h. Successful Locator Response

The AXN can now validate the valentine token and redirects the subject's browser to the Relying Party, returning a locator to the Relying Party that can be used to access the AXN Verified Attribute API for this particular interaction.

a. Verified Attribute Request

The Relying Party uses the locator in conjunction with the Valentine token and optionally a pre-configured API access token in an API request to the AXN for the verified attributes.

b. Verified Attribute Response

Actual verified attributes are returned to the Relying Party.

User Redirection Steps for Unknown AXN with API Calls

The full set of redirection steps and API calls are diagrammed below but the steps are not spelled out, as they are very similar to the steps shown in previous sections.

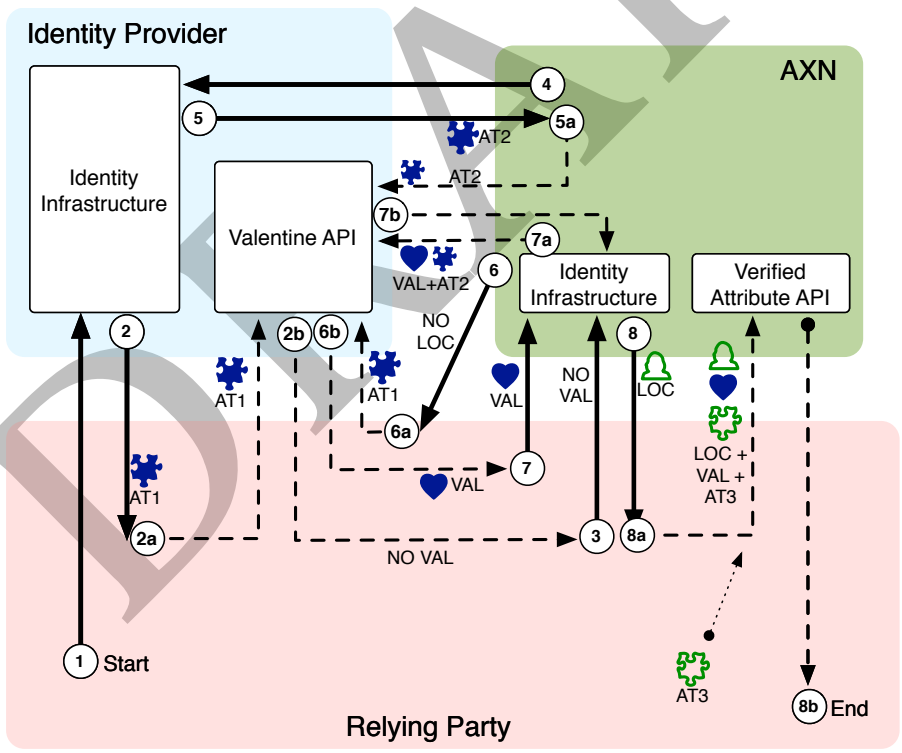


Figure 4: Unknown AXN Attribute Exchange with Redirects and API Calls

The steps shown in Figure 4 are as follows:

1. **Identity Assertion Request**

A request is made by the Relying Party to the Identity Provider to ascertain the identity of the subject and to obtain consent for the Relying Party to interact with the Identity Provider Valentine API.

2. **Identity Assertion Response**
   On successful authentication and authorization of the Relying Party, an OAuth 2.0 access token (AT1) will be returned to the Relying Party.
   a. **Valentine API Requests**
      The Relying Party asks for or queries the subject's Trusted AXN List
   b. **Valentine API Responses**
      The list or answer returned from the Identity Provider indicates that this particular AXN is not yet known/trusted by the subject.
3. **Empty Locator Request**
   The Relying Party redirects the subject's browser to the AXN, but cannot include the Valentine token, because the AXN is not yet trusted by the subject.
4. **Identity Assertion Request**
   A request is made by the AXN to the Identity Provider to obtain consent for the AXN to interact with the Identity Provider Valentine API.
5. **Identity Assertion Response**
   On successful authentication of the subject and authorization of the AXN as a trusted client within the attribute exchange context, the Identity Provider issues to the AXN an OAuth 2.0 access token (AT2)
   a. **Valentine API Requests (Trust List Insertion)**
      The AXN uses the AT2 access token to update or insert themselves into the subject's Trusted AXN List, thus enabling the Identity Provider to generate Valentine tokens.
6. **Empty Locator Response**
   The AXN redirects back to the Relying Party without a locator, so that the Relying Party can now fetch a Valentine token.
   a. **Valentine API Request(s)**
      The Relying Party again queries the subject's trusted AXN list and finds the AXN in the list. A Valentine token is requested.
   b. **Valentine API Response(s)**
      The Identity Provider returns a valentine token to the relying party.
7. **Locator Request with Valentine token**
   The Relying Party can now request a valentine token that is targeted to the AXN on behalf of the subject. The Relying Party again makes a Locator Request, this time including the valentine token.
1. **Valentine API Token Validation Request**
   The AXN submits the valentine token along with the AT2 access token to the Valentine API.
2. **Valentine API Response**
   The Identity Provider checks that AT2 represents the same subject as the valentine token and is targeted for the same client, the AXN. If this is true a positive validation result is returned.
8. **Successful Locator Response**
   The AXN can now validate the valentine token and redirects the subject's browser to the Relying Party, returning a locator to the Relying Party that can be used to access the AXN Verified Attribute API for this particular interaction.
   a. **Verified Attribute Request**
      The Relying Party uses the locator in conjunction with the Valentine token and optionally a pre-configured API access token in an API request to the AXN for the verified attributes.
   b. **Verified Attribute Response**
      Actual verified attributes are returned to the Relying Party.

Participation Requirements

Each participant has responsibilities in this system:

Identity Provider

- Must respond to Identity Assertion Requests with an access token (or a reference to retrieve an access token) that can be used to access the APIs listed below on behalf of the subject.

- Must maintain and manage a "trusted AXN list" that represents the subject's relationship with one or more AXNs.
- Must offer a "Valentine API" allowing a client to do the following:
  - Fetch a list of the subject's trusted AXNs
  - Generate and distribute a valentine token intended for an AXN on the trusted list
  - Validate a valentine token provided by an AXN
  - Update the trusted AXN list
- Must ensure that the user in some way knows and consents to allow a given participant to do any of the above activities

Relying Party

- Must have an existing relationship with one or more AXNs
  - Establishment of relationship is out of scope
- Must act as a relying party to make Identity Assertion Requests and validate Identity Assertion Responses from the IDP.
  - This may require a pre-existing relationship
- Must be able to interact as a client with the IDP Valentine API.
  - To request "read" access to trusted AXN list and access to request valentine tokens
  - To parse the list and determine whether any AXN on the list matches an AXN that the RP has a relationship to
  - To request a valentine token for that AXN
  - To pass the token onto the AXN
- Must be able to interact as a client with AXN Verified Attribute API.
  - To trigger a request for a Locator
  - To use the returned locator to securely retrieve verified attributes for the subject.

AXN

- Must have an existing relationship with one or more Relying Parties.
- Must act as a relying party to make Identity Assertion Requests to the IDP and validate Identity Assertion Responses from the IDP
  - This may require a pre-existing relationship
- Must be able to interact as a client with the Identity Provider Valentine API.
  - To request permission to update trusted AXN list and validate valentine tokens
  - To call the valentine validation API
  - To update the subject's trusted AXN list
- Must be able to issue a Locator which can be used to fetch verified attributes for the given subject and optionally within a given session context.
- Must offer an API allowing an RP acting as a client to do the following:
  - Request verified attributes
  - Fetch verified attributes

Constraints and Limitations

- Consent in this document is narrowly defined in this document to mean protocol level consent. This means that the subject is authorizing a client or relying party to interact with an Authorization Server or Identity Provider.
  - Some Identity Provider APIs also collect consent for attributes to be passed in federated identity tokens.
  - Consent for release of identity data beyond what is offered by the IDP is the full responsibility of the AXN and is out of scope of this document
- Communication between the AXN and Attribute Providers is expected to be proprietary and is out of scope of this document.
- Note that it is not required that each IDP and AXN publish identical APIs or use identical federated identity methodologies. Participants must simply provide equivalent functionality that is sufficiently secured, such that the sequence diagrams can occur.

- New participants are encouraged to closely follow API examples shown here, in hopes that a defacto API standard will evolve

Operational Recommendations

While not part of the protocol level interactions, the following recommendations are necessary for full certification of the trust framework specification

Security Considerations

User identity security is foremost in importance; a core objective is to reduce the opportunities for identity misuse on the Internet while enabling users to manage how their information is used by IDPs and RPs on the Internet. The AXN leverages a number of standard protocols across a secure Hypertext Transfer Protocol Secure (HTTPS) network connection. These include:

- **Whitelist,** is a list or register of entities that, for one reason or another, are being provided a particular privilege, service, mobility, access or recognition. All RPs, APs and IDPs that participate with the AXN are whitelisted, to ensure only authorized businesses are passed user verified claims.
- **User-Managed Access (UMA),** is a web-based access management protocol designed to give a web user a unified control point for authorizing who and what can get access to their online personal data (such as identity attributes), content (such as photos), and services (such as viewing and creating status updates), no matter where all those things live on the web.
- **Cross-Origin Resource Sharing** (**CORS**) is a web browser technology specification that defines ways for a web server to allow its resources to be accessed by a web page from a different domain.
- **System For Cross-Domain Identity Management (SCIM**) is a standard created to simplify user management in the cloud by defining a schema for representing users and groups and a REST API for all the necessary CRUD operations. In computer programming **create, read, update, and delete** (**CRUD**) are the four basic functions of persistent storage.
- **REpresentational State Transfer** (**REST**) is a style of software architecture for distributed systems such as the World Wide Web. REST has emerged as a predominant Web service design model.
- **OpenID** is an open standard that describes how users can be authenticated in a decentralized manner, eliminating the need for services to provide their own ad hoc systems and allowing users to consolidate their digital identities. Users may create accounts with their preferred OpenID IDPs, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication. The OpenID standard provides a framework for the communication that must take place between the identity provider and the OpenID acceptor (the RP) An extension to the standard (the OpenID Attribute Exchange) facilitates the transfer of user attributes, such as name and gender, from the OpenID identity provider to the relying party (each relying party may request a different set of attributes, depending on its requirements).
- **Open Standard For Authorization (OAuth)** allows users to share their private resources (e.g., photos, videos, contact lists) stored on one site with another site without having to hand out their credentials, typically supplying username and password tokens instead. Each token grants access to a specific site (e.g., a video editing site) for specific resources (e.g., just videos from a specific album) and for a defined duration (e.g., the next 2 hours). This allows a user to grant a third party site access to their information stored with another service provider, without sharing their access permissions or the full extent of their data.

A user's PII will not be stored at the AXN. The user will assert their attributes at RP sites to establish an account and procure services, and after completing their first verification flow, the user can easily leverage verified attributes to establish new RP accounts, thereby minimizing user friction and promoting adoption. Throughout this identity ecosystem, the user will be leveraging a credential (e.g., OpenID) issued and managed by their IDP which minimizes the use of passwords and reduces the friction associated with user account creation and log in.

The AXN design mitigates many potential threats by virtue of not creating a central data store of verified user attributes. In addition, security and privacy enhancing and protecting technology is built into the AXN infrastructure as follows:

- The implementation of AXN data flows uses Oauth 2.0, HTTPS for the transport layer, white lists to only allow registered IDPs, APs, RPs and users to access the AXN, and encryption techniques applied to data at rest
- OpenID is used for user credentials, AXN user account creation, and user access to the AXN is restricted to being available only via the user's registered IDPs and RPs
- User opt-in to each process control step associated with data collection, verification, and distribution of user attributes
- The use of out of band user verification methods (in addition to an IDP-issued OpenID) by the AXN to authenticate users as they access the AXN using their OpenID (only from IDPs and RPs registered with the AXN) such as SMS with a PIN, IP address, registered device ID, Biometric technologies, and Knowledge Based Access (KBA)
- The AXN user attribute data exchange with IDPs is limited to an encrypted token indicating that an attribute was verified and available with user consent via the AXN to participating RPs; and the actual verified user attributes are not provisioned directly to participating IDPs by the AXN
- Transport Layer Security (TLS) enables a secured connection, which is encrypted and decrypted with key material until the connection closes to prevent data eavesdropping and tampering.

Users will authenticate to their IDP to use their OpenID credential before initiating an account login with their RP. The AXN will create an account for each user, and will accept the OpenID credential as provisioned by the IDP. The AXN will also implement various verification services and methods that will generate claims associated with each user attribute. In all cases, participating RPs will consume the user asserted, verified attributes and associated claims to implement user authentication and authorization services prior to provisioning a user account and user access.

Application Hosting and Infrastructure

As a cloud service, the AXN doesn't require external systems to be provided by the customer for standard operations. Any RP or IDP-specific requirements for security or privacy should be readily accommodated. The AXN is designed to evolve and be maintained using standard software development methodologies. Any new requirements will be implemented as needed based on a thorough understanding of the customer requirements that are subsequently further refined into functional specifications for product development.

The AXN is designed to scale as needed. Resources are dynamically allocated based on loading requirements with expected uptime of 99+%. If the attributes are being verified for the first time, the entire verification flow can take between 2-3 minutes based on user response time. If the attributes are already verified by user for a different RP, it can be less than 10 seconds.

Identity Provider Valentine API Requirements

In an attribute exchange network, the Identity Provider has two new responsibilities: Attribute provider tracking and valentine token management. Attribute Provider tracking means that the Identity Provider manages a list for each subject that contains the set of AXNs (or single APs) that are authorized for use. Valentine token management is the process of issuing tokens that securely introduce a Relying Party to an AXN in the presence of a subject known to the Identity Provider. The Valentine API is the RESTful interface that allows interaction with both the Trusted AXN List and the Valentine token service.

Implementers playing the roles of RP and AXN must configure their solutions to interact with Identity Provider Valentine API. The Valentine API security model is described in this guide as using the OAuth 2.0 bearer token usage specification (RFC 6750), however the method by which the access token is actually requested may in fact be a specification other than the OAuth 2.0 Authorization Framework (RFC 6749).

The exact content and methods of the Valentine API will differ between Identity Providers, however the basic tasks should not. Relying Parties must be given a way to find out whether the AXN they deal with is trusted by the subject, and to request a valentine token in the case that the AXN is trusted; AXNs must be able to request that their AXN Identifier be added to the subject's Trusted AXN List, and must be able to submit a valentine token for validation.

Some implementations may combine interfaces to accomplish multiple tasks. An example of this combination might be a case where only the valentine token request interface is supplied to the relying party; an error returned

from that request would constitute a notification that the AXN is not in the subject's trusted AXN list. Another example of a permutation of this API could be a creation of AXN-specific scopes, such that the Identity Assertion Request for a given scope becomes analogous to a Trusted AXN List query, and the access token is either not issued or down-scoped if the subject does not have the particular AXN in the trusted AXN list. For the purposes of clarity, each task is separately documented in this guide.

Other valentine-related management duties are considered outside of the scope of this guide, for example the guide does not discuss how an Identity Provider might decide which AXNs are eligible for inclusion in the Trusted AXN List.

Overall Requirements

- The Identity Provider MUST document and run an API endpoint or endpoints for the following tasks:
  - Trusted AXN List Query
  - Per-Subject Trusted AXN List Enrollment
  - Valentine Token Generation
  - Valentine Token Validation
- The Identity Provider MUST protect Valentine API endpoints using bearer tokens that conform to the RFC 6750 IETF specification.
- The Identity Provider MUST provide an industry standard request mechanism for Relying Parties and AXNs to obtain RFC 6750 compliant access tokens.
- The Identity Provider SHOULD require subject consent prior to issuing an access token that is scoped for the Valentine API.
- The Identity Provider SHOULD provide a user interface through which the subject can view and revoke the access granted to both AXN and RP.
- The Identity Provider MUST protect the Valentine API using Transport Layer Security (TLS)

Security

- The validity window of the valentine token is RECOMMENDED to be no greater than 24 hours

Trusted AXN List Query Requirements

- The AXN MUST communicate in advance the list of AXN Identifiers that correspond to all supported Identity Providers.
- The Identity Provider MUST document a way in which the Relying Party can discover whether an AXN is on the Trusted AXN List of the subject of the presented OAuth 2.0 access token.
  - The Identity Provider MAY provide an interface for the RP to request a list containing the AXN Identifiers of zero or more AXNs with a relationship to the subject of the presented OAuth 2.0 access token.
  - The Identity Provider MAY provide an interface to allow an RP to request the status of a provided AXN Identifier.
  - The Identity Provider MAY specify an error code to be returned from the Valentine Token Generation Request to communicate that the requested AXN is not in the Trusted AXN List of the subject.
- The Identity Provider SHOULD limit read access to the Trusted AXN List to clients that have been authorized by the Subject.

Per-Subject Trusted AXN List Enrollment Requirements

- The Identity Provider MUST document a way in which an AXN can be added to the Trusted AXN List of the owner of the presented access token.
  - The Identity Provider MAY interpret a successfully authorized Identity Assertion Request for the Valentine API from a known AXN client ID as a request to enroll in the subject's Trusted AXN List.
  - The Identity Provider MAY publish an interface where the AXN Identifier is explicitly placed into the Subject's Trusted AXN List
- The Identity Provider MAY store information in the Trusted AXN List over and above the simple enrollment.

- The Identity Provider MUST ensure that only the AXN client id can request enrollment for the corresponding AXN Identifier.

AXN Identifier Format

It is an Identity Provider implementation decision as to how exactly the Relying Party determines whether a given AXN Identifier is on the subject's Trusted AXN List. The format of the AXN Identifier is also an Identity Provider Implementation decision. In the absence of an overriding architectural decision, this guide recommends that the Identity Provider allow the AXN to set a self-identifying URI as the AXN Identifier. In this case, the Relying Party should ensure that the domain of the AXN Identifier matches the domain of the URL that the Locator Request is sent to.

Valentine Token Generation Requirements

- The Relying Party MUST specify a target AXN Identifier when making a valentine token generation request.
- If the Identity Provider generates a valentine token, the token MUST have the following characteristics:
    - The target AXN MUST be on the Subject's Trusted AXN List
    - The valentine token MUST be explictly scoped for the specified target AXN
    - The valentine token MUST be delivered to a Relying Party authorized for the

- The Identity Provider MUST only accept valentine token generation requests that include a single AXN Identifier as the target.
- The Identity Provider MUST only return the generated valentine token to the requesting client if the requested AXN Identifier is present in the Subject's Trusted AXN List
- If the Identity Provider uses pairwise pseudonymous subject identifiers and includes a Subject identifier in the Valentine token, that subject identifier is RECOMMENDED to be encrypted to prevent leakage of information to the Relying Party
- The Identity Provider MAY encrypt the entire valentine token to keep all parties from introspecting the token independently.

Valentine Token Validation Requirements

- The Identity Provider MUST return a failure status under the following conditions:
    - If the OAuth 2.0 Access token used to authorize API access does not belong to the user for whom the Valentine token was generated
- The AXN MUST ignore unrecognized fields in the Valentine Token

Use Limitations

- The AXN MUST NOT attempt to validate the valentine token if a subject identifier is present in the valentine token and that subject identifier does not match the subject identifier returned from the Federated Identity Assertion.

Identity Provider Valentine API Authentication

Both the Relying Party and the AXN must obtain OAuth access tokens that represent the user present in the browser to be able to access the Identity Provider Valentine API. To get these two items, both the Relying Party and the AXN must each in turn redirect the subject to the Identity Provider, making an identity assertion request. If the subject is already authenticated and has already consented to allowing the RP and AXN to act as a client, the Identity Provider may respond to the identity assertion request without displaying anything visible to the subject, instead transparently including in the identity assertion response either the actual assertion containing the data directly, or a pointer to retrieve the identity assertion from an API. If however the user is not already authenticated at the Identity Provider or consent needs to be collected, the user will be prompted.

The identity assertion request described above may be implemented in a number of industry standard ways. Identity standards such as OpenID 2.0, OAuth 2.0, OpenID/OAuth Hybrid or OpenID Connect are examples of industry best practice ways to securely request attribute information across domains.

Any of the above listed standards may be used in an AXN flow. More detailed requirements are listed below.

Note: This section does not discuss how the **subject** authenticates – it is assumed the mechanism for validating the identity of the user is wholly the responsibility of the Identity Provider and is out of scope for this document. This section is meant to describe how either an RP or an AXN, acting as a **client** can make a federated identity request and receive attributes back that identifies the subject and enables the client to act in a **delegated capacity** on behalf of the subject while making API requests to the Identity Provider Valentine API.

Valentine API General Requirements

Security

- The identity assertion request destination URL MUST be protected by Transport Layer Security (TLS).
- The Identity Provider SHOULD obtain consent from the subject to release identity information.

Identity Provider Requirements

- The Identity Provider MUST publish at least one standards-based method to make an Identity Assertion Request and provide federated responses upon successful request.
- Upon successful authorization of Valentine API scopes during an identity assertion request, the Identity Provider SHOULD return an access token to the client.
- If an Identity Provider returns identity attributes to the client, the identity attributes MUST be signed

Client Credentials

- The Identity Provider MAY require that the RP and AXN pre-register a client identifier and/or client secret.
- The Identity Provider MAY issue credentials to be used by the RP and AXN when making Identity Assertion Requests.

Identity Assertion Request

OpenID 2.0

- Identity Providers providing an OpenID 2.0 Federated Identity service:
  - MUST conform to the OpenID 2.0 Specification where applicable
  - MAY conform to the OpenID 2.0 PAPE Specification
  - MUST perform RP Discovery

OAuth 2.0

- Identity Providers providing an OAuth 2.0 Federated Identity service:
  - MUST conform to RFC 6749 and 6750 where applicable
  - MAY provide a request using the code response type
  - MAY provide a request using the token response type

OpenID Connect

- Identity Providers providing an OpenID Connect Federated Identity service:
  - MUST conform to the OpenID Connect Messages spec at http://openid.net/connect

Verified Attribute API Requirements

The API by which the AXN communicates data to the RP is expected to most commonly be a read-only RESTful API, and the recommended design pattern for data request and response is a SCIM 1.1 resource request. Other methods for requesting and receiving attributes are acceptable, provided they comply with the Requirements listed below.

From a Relying Party perspective, there are two different sets of considerations for consuming from the verified attribute API that correspond to the type of data consumed. Those two design patterns are discussed below as the "synchronous" and "asynchronous" consumption models.

Overall Requirements

Security

- Verified attribute API endpoints MUST be protected by TLS
- It is RECOMMENDED to use RFC 6750 to protect verified attribute APIs
- Attributes offered by a verified attribute API SHOULD be limited to one-time use only
    - Exact details of attribute consumption are contractual
- Data availability of attributes via the API SHOULD have a tightly time-limited expiry date
    - Lifetime of data availability is RECOMMENDED not to exceed 15 minutes
- If verified attribute data passes via the browser it MUST be encrypted

Content

1. It is the AXN's responsibility to ensure that only the minimum set of data requested by the Relying Party is available via the Verified Attribute API.
2. It is the AXN's responsibility to ensure that once the published expiry date has passed for the data, the Verified Attribute API returns an appropriate error.

Protocol

It is RECOMMENDED for the AXN to use the SCIM 1.1 REST API protocol to request and retrieve verified attributes

- SCIM 1.1 REST API documentation can be found at http://datatracker.ietf.org/doc/draft-ietf-scim-api
- The AXN MUST support the GET verb as per SCIM 1.1 section 3.2.2
- The AXN SHOULD NOT support data modification or deletion verbs such as PATCH or DELETE
- The RP SHOULD be able to request user data based on the subject identifier

Client Authentication

- The AXN MUST require an HTTP Authorization header on all calls to verified API endpoints.
- THE AXN MAY accept either HTTP basic credentials or RFC 6750 OAuth 2.0 tokens to authenticate clients.

API Security via RFC 6750

If the AXN is using RFC 6750 (OAuth 2.0) to protect the verified attribute API:

- The AXN SHOULD use the 'code' response type
- The AXN SHOULD issue refresh tokens
- The validity window of any OAuth token SHOULD NOT exceed the average data availability lifetime

Verified Attribute API Authentication

There are a number of ways that access to the Verified Attribute API can be secured. This is largely an implementation decision on the part of the AXN, and while a standards-compliant design pattern has been documented below as an example for technicians wanting to at least be given a starting point, the actual mechanism used is dictated by the AXN and could take many forms. Regardless of the mechanism by which the API is secured, the following requirements apply:

General Requirements

1. The API MUST be protected using Transport Layer Security (TLS)
2. Each Relying Party MUST be issued unique client credentials to access the Verified Attribute API
3. The AXN MUST publish an expiry date for the verified attribute data available from the Verified Attribute API
4. The AXN MAY publish a one-time-access policy for the Verified Attribute API

AXN Requirements

1. The AXN MUST NOT return an API URL that contains within the URL string any personally identifying or confidential information
2. The AXN MUST NOT return verified attributes to the Relying Party if the Relying Party attempts to access the data after the published expiry date

Relying Party Requirements

If the AXN publishes a one-time-access policy for the Verified Attribute API, or if the expiry date for a given set of verified attributes has expired, an RP needing to re-consume verified attributes subsequent to first access MUST NOT make a call to the Verified Attribute API, but instead retrieve a new Valentine token for that user, re-engaging with the AXN for "fresh" attributes.

AXN Locator Request

Once a relying party has accessed the subject's list of trusted AXNs, the relying party must redirect the subject's browser to the AXN. Note that this redirection can occur in one of two circumstances:

- The AXN identifier was found in the subject's trust list
  - In this case, the relying part will be passing a valentine token as part of the redirect
- The AXN identifier was not found in the subject's trust list
  - In this case, the relying party is considered to be introducing a new subject to the AXN. No valentine token can be passed, and the AXN must work with the subject to be added to the trust list before continuing

Depending on the implementation, the redirection of the RP to the AXN may either occur as part of a token request for access to the Verified Attribute API or as a standalone redirection. Either implementation is supported but the following requirements must be followed.

AXN Requirements

- The redirection target URL MUST be protected by Transport Layer Security (TLS)
- The AXN MUST take reasonable measures to identify the referring party as being a valid Relying Party

Relying Party Requirements

- The Relying Party MUST submit a unique client credential as part of the request
- The Relying Party MAY also submit a client secret or other means to directly authenticate
- The Relying Party SHOULD NOT include the valentine token directly in the target URL

AXN Locator Response

In the case where the Valentine token validates, and the subject successfully interacts with the AXN such that verified attributes can be produced and made available to the Relying Party, the AXN SHOULD return a response to the Locator Request that includes a Locator value.

The Locator is a reference that can be used to call a specific REST API location in the Verified Attribute API. The format, lifespan and meaning of the Locator is specific to the implementation – it may represent a static reference to a subject, or it may represent an ephemeral reference to a subject within a specific context and timeframe. Communication of the locator's format, cardinality and meaning is done out of band and is not within the scope of this document.

AXN Locator and Locator Response Requirements

1. The value of the Locator MUST NOT itself contain personally identifiable information
2. The Locator Response MUST be protected by Transport Layer Security (TLS)
3. A Locator MUST only be sent if the access token AT2 has been successfully requested from the Identity Provider
4. A Locator MUST only be sent if the Identity Provider successfully validates the Valentine token

Detailed Protocol Sequences

Legend:

- Dotted lines represent backchannel (no browser present)
- Solid lines represent front channel (browser present)

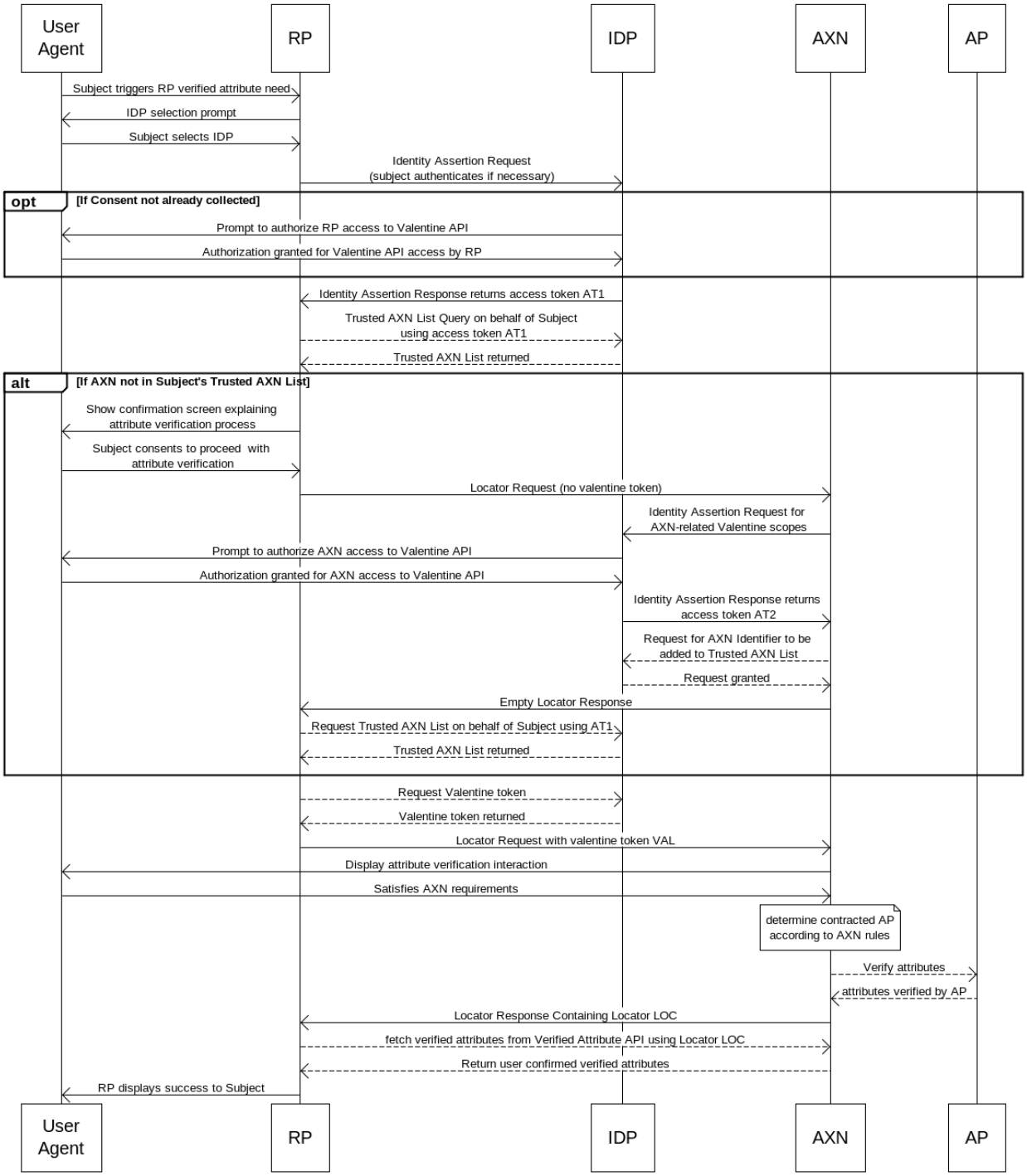


Figure 5 : First Time User Enrolling With RP and AXN

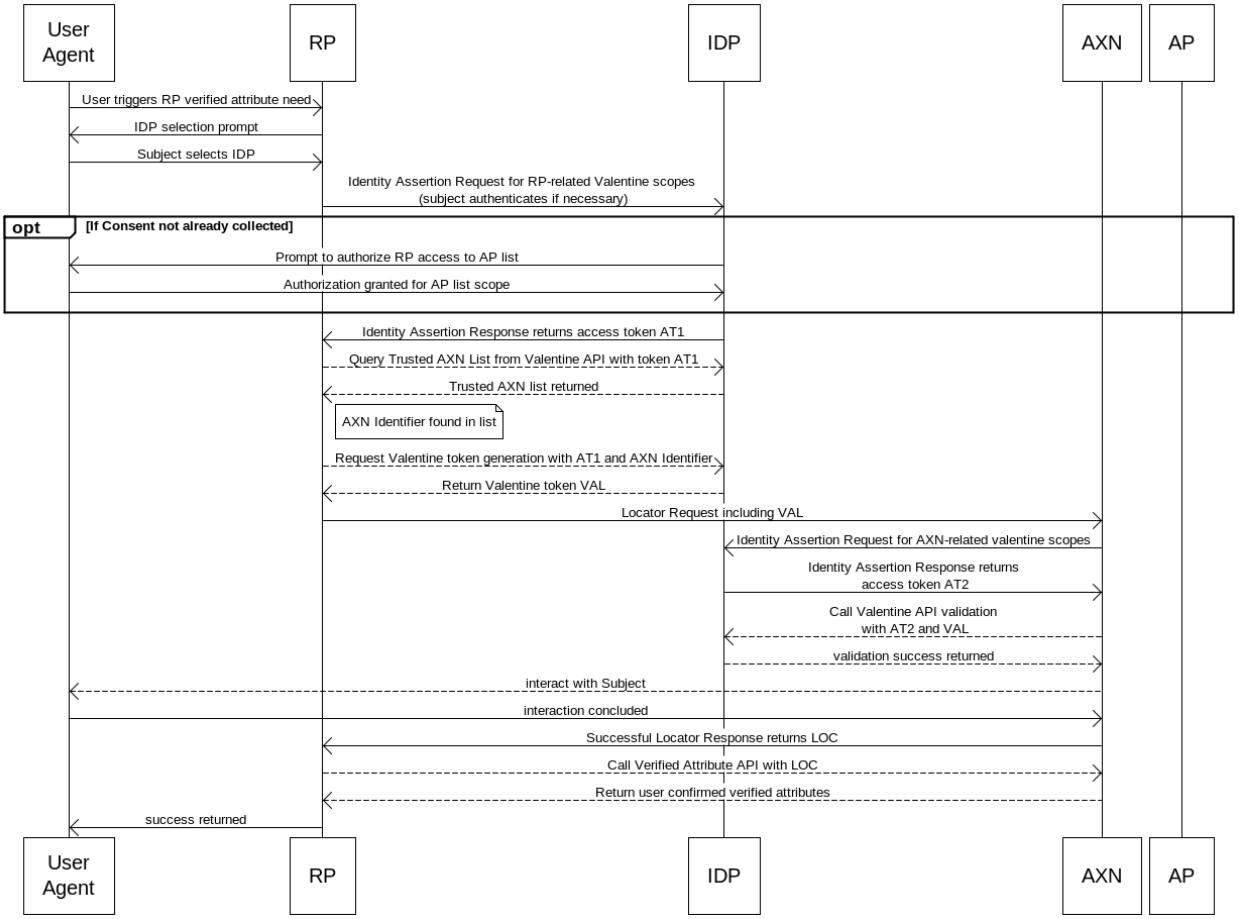


Figure 6 : Existing AXN User Interacting with RP

Design Pattern Recommendations

Many of the choices implementers can make while interacting with an AXN have more to do with the implementer's core business than with the process of communicating verified attributes across domains. The examples in this section detail how some AXN members have constructed their implementation, and are intended to show what could be done. This section is meant to inform a new implementer on what kinds of information they may wish to construct, or what kinds of data may be seen from partners.

Identity Provider Patterns

Valentine Token Construction

- Valentine Token MAY be constructed in the following way:
  - Format must be a signed JWT as per the JOSE specification
- Valentine Token MAY contain the following information:
  - Issuer: an identifier or endpoint that identifies the Issuer
  - Issue Time: the time that the valentine was issued
  - Expiry: the time after which the Valentine is no longer valid
  - RP ID: the clientid of the requesting RP
  - AXN ID: the clientid of the requested AXN
- Exact field names will vary by Identity Provider
- Identity Providers MAY include additional fields unique to their processing needs

Token Audience

The Valentine Token is constructed by the Identity Provider and eventually validated by the Identity Provider. In some implementations, this is literally interpreted in the token as the issuer and audience attributes having the same value. In such a case, the AXN ID may be absent, may be placed in a custom attribute, or may be listed in the audience attribute in addition to the original issuer of the token in an array. Other implementations may define the RP ID as the "authorized party" and the AXN ID as the "intended audience", and simply consider the ultimate audience (the issuer) as implied.

Example Valentine Token

Example Signed & Encoded Token (sequences abbreviated):


```
{
  "token":"eyJhbGci…pXVCJ9.eyJhdWQiOiJhbzF…XFsenZCQ3lsU0EifQ.XaAa4a6MTi…ixnETzkmY
0fw",
  "scope":"",
  "expires_in":86400
}
```


Header

Body

Signature

Example Token Header After Decoding

Header


```
{
 "alg":"RS256",
```

```
 "typ":"JWT"
}
```

Example Valentine Token Body After Decoding

Sequences are shortened

```
Body
{
 "aud":"ao1fd5uyaI9j6xoe",
 "exp":86400,
 "iat":1360610851,
 "iss":"https://axn.screenname.aol.com",
 "_aol":"T2JPIraVIKK930yrjgZE16TL4i_4YotDTl-
gi5ChLZ4iOzXIoeqRSINryPqt1Zr9INx6Nffkguicm5b…6O99d87RTYqlzvBCylSA"
}
```

Trusted AXN List Content Example

The Trusted AXN List is a per-user list maintained by the Identity Provider. Exact content of the AXN List is an implementation detail however it is strongly recommended that implementers begin to harmonize the implementation details in this area.

AXN Identifiers

The AXN Identifier listed on the Trusted AXN List is owned by the Identity Provider, and may be defined differently for different Identity Providers.

The AXN must communicate which identifier should expected by the Relying Party for each supported Identity Provider.

> For example, AXN “A” may appear on the Trusted AXN List of Google as a guid, while the same AXN could appear on the Trusted AXN List as “AXN-A-CLIENTID”.

Attribute Network Patterns

Example SCIM Data Payload

Each AXN will publish the schema of attributes that they will publish, and then make those attributes available via API. Here is an example of a JSON object delivered via SCIM that an AXN might want to construct to communicate data coming from multiple backend Attribute Providers:

```
        {
provider:"ATTRIBUTES R US",
"attributes":
 {"homePhone":"5555551201",
 "provider":"ATTRIBUTES R US",
 "verification":”authoritative”,
 "attributeType":"Telephone",
 "dateCreated":1365542498645,
 "dateVerified":1365542498643
 },
 {"billAddress":"432 MAIN STREET, MYTOWN, ST 21100",
 "provider":"ATTRIBUTES R US",
 "verification":”third party”,
 "attributeType":"Address",
 "dateCreated":1365542498645,
 "dateVerified":1365542498643
```

```
        },
                        {“phoneAddressMatch”:true,
                        “provider”:”ATTRIBUTES R US”,
                        “verification”:”authoritative”,
                        “attributeType”:”attributeMatch”,
                        "dateCreated":1365542498645,
   "dateVerified":1365542498643
                        },
},
{
  provider:"DEVICE SYSTEMS, INC",
  "attributes":
   {"Device":"t6jmg94u90348fg0912",
   "provider":"DEVICE SYSTEMS, INC.",
   "verification":”directCapture”,
   "attributeType":"Device ID",
   "dateCreated":1365542498645,
   "dateVerified":1365542498643
                        }
        },
        {
         provider:"INFORMATION INTERSECTION",
  "attributes":
   {"ssnDobMatch":true,
   "provider":"INFORMATION INTERSECTION",
   "verified":”third party”,
   "attributeType":"attributeMatch",
   "dateCreated":13655424914535,
   "dateVerified":13655425548643
                        }
        }
```

TIG Appendix A: Identity Provider API Examples

The Attribute Exchange Network (AXN) API for Identity Providers (IDP) is built on the foundation of Google's Street Identity API, and provides functionality for Relying Parties (clients) and Service Providers by exposing three endpoints: Discovery Endpoint, Token Endpoint and Token Info Endpoint.

Discovery Endpoint allows Relying Parties to discover Service Providers that have been authorized by users at an IDP (e.g., Google, AOL, Verizon) for a specific purpose - e.g., to act as sources of some trustworthy information. An example of a Service Provider is an application that can provide a verified street address of the user. Relying Parties can discovery such a Service Provider using Street Identity API if the user has authorized the Service Provider for a specific scope (in this case - the https://www.idpapis.com/auth/streetidentity.write scope). The AXN version still enables this functionality, but simplifies the transactions and user experience by serving as a conduit for multiple Service Providers and Attribute Providers.

The Token Endpoint allows Relying Parties to obtain access tokens that can be later used to access information or use services provided by Service Providers.

Service Providers can use the Token Info Endpoint to validate tokens that these providers receive from Relying Parties.

Google Street Identity

The Google Street Identity API can be used as a Valentine API. The section here refers to the Google API as of 12 December 2013, please refer to the official Google Documentation at time of implementation to confirm that no changes have been made.

Relying Parties can use the Discovery Endpoint (/discovery) and Token Endpoint (/token). Service Providers can use the Token Info (/tokeninfo) endpoint, which supports HTTP GET and HTTP POST methods.

discovery	Retrieves a map of scopes and lists of authorized Service Providers for these scopes.
token	Retrieves a response containing an issued signed JWT token for a specific Service Provider.
tokenInfo	Validates a signed JWT token and returns token information. Clients can use either HTTP GET or POST methods.
storeData	Stores or updates user data in an encrypted token that is created by the AXN.
fetchData	Retrieves user data related encrypted for subsequent usage.

discovery Endpoint

- Requires authorization
- Retrieves a map of scopes and lists of authorized Service Providers for these scopes.

The Discovery Endpoint is exposed by Google for Relying Parties (RP). Discovery Endpoint allows RP to obtain the list of clientIds of Service Providers (SP) that have been authorized by a particular user of Google for a specific set of Street Identity related scopes. Currently, these scopes are:

- https://www.idpapis.com/auth/streetidentity.write
- https://www.googleapis.com/auth/verifiedage.write
- https://www.googleapis.com/auth/verifiedgender.write

- The RP, as the client of this endpoint, obtains information about "read" type scopes, however, which may be one of the following:
  - https://www.idpapis.com/auth/streetidentity.read
    https://www.googleapis.com/auth/verifiedage.read
  - https://www.googleapis.com/auth/verifiedgender.read

For example, if there is a Service Provider that has obtained authorization for the https://www.idpapis.com/auth/streetidentity.write scope then the RP would obtain this clientId in the list for https://www.idpapis.com/auth/streetidentity.read scopes. See further explanation in this section.

Request

HTTP Request

GET https://www.idpapis.com/streetidentity/discovery

Optional Parameters

Property Name	Value	Description
Scope	string	Space-delimited list of scopes for which lists of Service Providers should be returned.

Authorization

This request requires authorization with at least one of the following scopes.

Scope
https://www.idpapis.com/auth/streetidentity.read
https://www.googleapis.com/auth/streetidentity.read
https://www.googleapis.com/auth/verifiedgender.read

Request Body

Do not supply a request body with this method.

Response

If successful, this method returns a response body with the following structure:

```
{
 "https://www.googleapis.com/auth/streetidentity.read": [
  string
 ],
 "https://www.googleapis.com/auth/verifiedage.read": [
  string
 ],
 "https://www.googleapis.com/auth/verifiedgender.read": [
  string
 ]
}
```

Property Name	Value	Description
https://www.googleapis.com/auth/streetidentity.read[]	list	List of clientIds of Service Providers that have been authorized for the "streetidentity.write" scope. The "streetidentity.write" scope is a superset of the "streetidentity.read" scope. The client that makes the discovery should only be concerned with understanding the "read" type scope. This field is optional in the response returned to the client and is not included if the request was not authorized for the "streetidentity.read" scope or if there were no Service Providers authorized by the user for the matching "streetidentity.write" scope.
https://www.goog	list	List of clientIds of Service Providers that have been authorized for the

leapis.com/auth/verifiedage.read[]		"verifiedage.write" scope. The "verifiedage.write" scope is a superset of the "verifiedage.read" scope. The client that makes the discovery should only be concerned with understanding the "read" type scope. This field is optional in the response returned to the client and is not included if the request was not authorized for the "verifiedage.read" scope or if there were no Service Providers authorized by the user for the matching "verifiedage.write" scope.
https://www.googleapis.com/auth/verifiedgender.read[]	list	List of clientIds of Service Providers that have been authorized for the "verifiedgender.write" scope. The "verifiedgender.write" scope is a superset of the "verifiedgender.read" scope. The client that makes the discovery should only be concerned with understanding the "read" type scope. This field is optional in the response returned to the client and is not included if the request was not authorized for the "verifiedgender.read" scope or if there were no Service Providers authorized by the user for the matching "verifiedgender.write" scope.

token Endpoint

- Requires authorization
- Retrieves a response containing an issued signed JWT token for a specific Service Provider.

Request

HTTP Request

POST https://www.idpapis.com/streetidentity/token

Required Parameters

Property Name	Value	Description
client_id	string	Client ID of the Service Provider for which token should be issued.

Optional Parameters

Property Name	Value	Description
Scope	string	Scope for which token should be issued.

Authorization

This request requires authorization with at least one of the following scopes

Scope
https://www.googleapis.com/auth/verifiedage.read
https://www.googleapis.com/auth/streetidentity.read
https://www.googleapis.com/auth/verifiedgender.read

Request Body

Do not supply a request body with this method.

Response

If successful, this method returns a response body with the following structure:

```
{
 "token": string,
 "expires_in": integer,
```

```
  "scope": string
}
```

Property Name	Value	Description
token	string	Signed Service Token (JWT). Signing is done according to the JSON Web Signature (JWS) standard. The signed token has the following structure: {base64urlenc_header}.{base64urlenc_jsonpayload}.{base64 urlenc_sig}
expires_in	integer	The expiry time of the token, as number of seconds left until expiry.
scope	string	Space-delimited list of scopes for which the token is authorized.

tokenInfo Endpoint

Validates a signed JWT token and returns token information. Clients can use either HTTP GET or POST methods.

Request

HTTP Request

GET|POST https://www.idpapis.com/streetidentity/tokeninfo?key={API_KEY}

Required Parameters

Property Name	Value	Description
Token	string	Signed JWT token that should be validated

Request Body

Do not supply a request body with this method.

Response

```
{
  "issuer": string,
  "audience": string,
  "issued_to": string,
  "user_id": string,
  "scope": string,
  "issued_at": long,
  "expires_at": long
}
```

Property Name	Value	Description
Issuer	string	The URL of the Street Identity API Token Endpoint
Audience	string	Client ID of the Service Provider for which the token was issued
issued_to	string	Client ID of the Relying Party to which the token was issued.
user_id	string	Obfuscated GAIA user ID for which the attribute token was issued.
Scope	string	Space-delimited list of scopes for which the token is authorized.
issued_at	long	Epoch time when the token was issued.

expires_at	long	Epoch time when the token expires.

storeData Endpoint

- Requires authorization
- Stores user related encrypted data token.

Request

HTTP Request

POST https://www.idpapis.com/streetidentity/storeData

Parameters

Property Name	Value	Description
userData	String	User data related encrypted token

Authorization

This request requires authorization with at least one of the following scopes

Scope
https://www.idpapis.com/auth/userdata

Request Body

Do not supply a request body with this method.

Response

If successful, this method returns a response body with the following structure:

```
{
  "response": string
}
```

Property Name	Value	Description
response	String	Success/Failure

fetchData Endpoint

- Requires authorization
- Retrieves user related encrypted data token.

Request

HTTP Request

GET https://www.idpapis.com/streetidentity/fetchData

Parameters

Do not supply any request parameters with this method.

Authorization

This request requires authorization with at least one of the following scopes

Scope
https://www.idpapis.com/auth/userdata

Request Body

Do not supply a request body with this method.

Response

If successful, this method returns a response body with the following structure:

```
{
  "userData ": string
}
```

Property Name	Value	Description
userData	String	User data related encrypted token

TIG Appendix B: Web Sequence Diagram Scripts

The sequence diagrams used in this document are generated at http://websequencediagrams.com. To alter or improve the existing diagrams, copy the scripts below into the left side of the screen. Some script features require the use of the paid version of the website.

Script 1: First time user enrolling with RP and AXN

```
participant "User\nAgent" as user
participant RP as rp
participant IDP as idp
participant AXN as axn
participant AP as ap

user->rp:Subject triggers RP verified attribute need
rp->user:IDP selection prompt
user->rp: Subject selects IDP
rp->idp:Identity Assertion Request\n(subject authenticates if necessary)
opt If Consent not already collected
idp->user:Prompt to authorize RP access to Valentine API
user->idp:Authorization granted for Valentine API access by RP
end
idp->rp:Identity Assertion Response returns access token AT1
rp-->idp:Trusted AXN List Query on behalf of Subject\n using access token AT1
idp-->rp: Trusted AXN List returned

alt If AXN not in Subject's Trusted AXN List
  rp->user:Show confirmation screen explaining\n attribute verification process
  user->rp: Subject consents to proceed  with\n attribute verification
  rp->axn:Locator Request (no valentine token)
  axn->idp:Identity Assertion Request for\n AXN-related Valentine scopes
  idp->user:Prompt to authorize AXN access to Valentine API
  user->idp:Authorization granted for AXN access to Valentine API
  idp->axn:Identity Assertion Response returns\n access token AT2
  axn-->idp:Request for AXN Identifier to be\n added to Trusted AXN List
  idp-->axn: Request granted
```

```
  axn->rp: Empty Locator Response
  rp-->idp: Request Trusted AXN List on behalf of Subject using AT1
  idp-->rp: Trusted AXN List returned
end
rp-->idp: Request Valentine token
idp-->rp: Valentine token returned
rp->axn: Locator Request with valentine token VAL
axn->user:Display attribute verification interaction
user->axn:Satisfies AXN requirements
note over axn:determine contracted AP\n according to AXN rules
axn-->ap:Verify attributes
ap-->axn:attributes verified by AP
axn->rp:Locator Response Containing Locator LOC
rp-->axn : fetch verified attributes from Verified Attribute API using Locator LOC
axn-->rp:Return user confirmed verified attributes
rp->user:RP displays success to Subject
```

Script 2: Existing AXN user enrolling services at RP

```
participant "User\nAgent" as user
participant RP as rp
participant IDP as idp
participant AXN as axn
participant AP as ap

user->rp:User triggers RP verified attribute need
rp->user:IDP selection prompt
user->rp: Subject selects IDP
rp->idp:Identity Assertion Request for RP-related Valentine scopes \n(subject authenticates if necessary)
opt If Consent not already collected
  idp->user:Prompt to authorize RP access to AP list
  user->idp:Authorization granted for AP list scope
end
idp->rp:Identity Assertion Response returns access token AT1
rp-->idp:Query Trusted AXN List from Valentine API with token AT1
idp-->rp: Trusted AXN list returned
note right of rp: AXN Identifier found in list
rp-->idp: Request Valentine token generation with AT1 and AXN Identifier
idp-->rp: Return Valentine token VAL
rp->axn:Locator Request including VAL
axn->idp:Identity Assertion Request for AXN-related valentine scopes
idp->axn:Identity Assertion Response returns\n access token AT2
axn-->idp:Call Valentine API validation\n with AT2 and VAL
idp-->axn:validation success returned
axn-->user: interact with Subject
user->axn: interaction concluded
axn->rp: Successful Locator Response returns LOC
rp-->axn : Call Verified Attribute API with LOC
axn-->rp:Return user confirmed verified attributes
rp->user:success returned
```