ATTRIBUTE EXCHANGE NETWORKS: NEW INFRASTRUCTURE FOR DIGITAL BUSINESS

Introducing the OIX Attribute Exchange Trust Framework

AXN White Paper

THE OPEN IDENTITY EXCHANGE | LOCKSTEP CONSULTING

By Steve Wilson, Lockstep Consulting

Version 1.2
October 2013

Executive Summary

A defining image of the digital age is the Internet dog. At the dawn of e-commerce, Peter Steiner's famous 1993 New Yorker cartoon highlighted that we can't easily tell who or what we're dealing with online. Trust and identity have been inexplicably linked as the core concerns of Internet businesses, network service providers, technologists and regulators.

Now the digital economy is taking shape and mainstream industries are moving with confidence online, we are starting to deal with others in cyberspace with more nuance. Until recently, online risks have been hard to quantify. When there is no solid experience of what might go wrong in a new business environment, identification becomes a sort of safety net. We feel the need to know all we can about a stranger before we feel safe doing business with them. Yet we've learned the hard way that piling on more and more identification data is no recipe for success, for it only fuels identity theft and cybercrime. What's more, we may recall that in traditional business we do very well with incremental identification appropriate for the transaction at hand, without needing to know everything about the other person.

Attributes are the currency of e-business. For efficiency, privacy and legal simplicity, parties to transactions generally apply the need-to-know principle: what do you need to know about someone in order to deal with them? The answer varies from case to case, and includes such attributes as professional registration or license number, organisation and department, staff ID, security clearance, customer reference number, credit card number, unique health identifier, allergies, blood type, social security number, address, citizenship status, social networking handle, pseudonym and so on. Digital business has matured to the point where the proper focus of authorization can shift to attributes.

In different contexts we need to know different things about our customers, users, providers and partners. For instance, we know very little about the accountant who does our taxes, or the pharmacist who dispenses our medicines. Moreover the pharmacist probably knows almost nothing about the doctor who wrote our prescription – except for their healthcare registration details. What's going on here to enable high levels of trust in the most sensitive situations with only marginal identification? The key is, in routine business, particular *attributes* about our fellow users are just as important – if not more so – than identity. This realization lies behind the *Attribute Exchange Network*, an architecture and governance framework developed by the Open Identity Exchange Foundation.

The OIX Attribute Exchange (AXN) Trust Framework Specification is a comprehensive master plan for implementing identity as a service infrastructure for the real time sharing of precise authority information across all digital business settings. The AXN is user-centric and privacy enhancing in that it provides for user control of fine grained and permissioned exchange of attributes and verification of those attributes. The Specification leverages the latest federated identity standards and protocols, and frames all necessary business, legal, technological, privacy policy and assurance arrangements. The vision is that private and public sector businesses and consortia can implement AXN infrastructure fit for their purposes in their own environments. Thus a range of organisations both old and new will be able to serve up standardised attribute information for the benefit of Relying Parties, bringing the benefits of federation to more end users than ever before.

Table of Contents

1. Attributes: The "Currency" of e-Business

The Attribute Exchange Network was developed by the Open Identity Exchange (OIX) to help build a new world, where individuals can conduct sensitive business transactions safely online without needing to deal with scores of passwords. In the near future, organizations will more efficiently do business online by trusting the identities and credentials provided by others. Redundant processes associated with managing and testing identity data will be streamlined; fraud losses will be cut; new services previously deemed too risky will be provided online with the sort of confidence long taken for granted in the physical world.

In different contexts we need to know different things about our customers, users, providers and partners. For instance, we know very little about the accountant who does our taxes, or the pharmacist who dispenses our medicines. Moreover the pharmacist probably knows almost nothing about the doctor who wrote our prescription – except for their healthcare registration details. What's going on here to enable high levels of trust in the most sensitive situations with only marginal identification? The key is, in routine business, particular attributes about our fellow users are just as important – if not more so – than identity. This realization is behind the Attribute Exchange Network, an architecture and governance framework developed by the Open Identity Exchange Foundation.

Attributes are the currency of transactional business; they are how we can tell that a counter party is authorized to deal in the transaction at hand. For instance, a merchant needs to know a shopper's credit card number more than anything else (and according to the goods involved, the billing address and perhaps the customer's age will be important too); a pharmacist doesn't need to know anything more about a doctor writing a script than their prescriber number; a controlled children's social networking service will need to know that a member is under-age; a consultative health chat room may desire that anonymous users nevertheless have the conditions of interest; and a drug company running a clinical study must be sure of participating patients' and investigator's trial IDs while keeping their identities secret.

Despite the centrality of attributes in routine business, until recently there was no agreed way to confer attribute information digitally. Instead, since the dawn of e-commerce, authentication management has tended to look to more abstract identity constructs for establishing "trust". The result has been arguably rather coarse. Rather than trying to match the fine-grained attribute information needed to authorize different transactions, conventional identity and access management systems tend to over collect Personally Identifiable Information, cache authorization information in appropriate places, and because they don't

directly engage authoritative sources, tend to suffer from incomplete, inaccurate or obsolete data.

In contrast, efficient, automated attribute exchange via an AXN brings:

- enhanced privacy as a result of tighter disclosure of personal information germane to the context, and less exposure of extraneous data
- simpler liability arrangements and lower legal costs, because it is more straightforward to vouch for concrete attributes than abstract identity
- smoother deployment of large digital projects through better preservation of context and the ways people deal with one another in each business setting.

Acknowledgements

This white paper would not have been possible without the support of the UK IDA alpha and beta teams, and OIX Foundation management. Special thanks go to David Coxe (ID / DataWeb), David Rennie (UK Government Identity Assurance Program), Rob Laurence (Innovate Identity) and Don Thibeau (OIX).

Further, we are all indebted to the organisations and individuals that contributed via Working Groups to the development and publication of the AXN Trust Framework Specification; these people are acknowledged in the Appendix.

2. About the Open Identity Exchange

The Open Identity Exchange (OIX) has its roots in the early days of the Obama administration, when the US General Services Administration (GSA) was tasked with identifying how to leverage open identity technologies for better interaction by the American public with government services in healthcare, taxation and social security. In 2009 the GSA struck a public/private partnership with the Open ID Foundation (OIDF) and the Information Card Foundation (ICF) focused on the legal and policy basis needed to support Open ID transactions. The partnership eventually developed a *trust framework model*. A Joint Steering Committee was then constituted amongst ODF and ICF members, to select implementation options for the framework. As momentum grew, the US CIO recommended the formation of a non-profit corporation, the Open Identity Exchange (OIX). In 2010, the OIX was incorporated, through grants from

OIDF and ICF.[1] OIX was the first trust framework provider certified by the US Government.

The core business of the OIX is the development, sponsorship and promotion of *Trust Frameworks* to improve the conduct of digital business. According to OIX principles, a *Trust Framework* is an ensemble of tools, rules and business policies that enable parties within a "community of interest" processing digital identity credentials to trust the identity, security, and privacy policies of the credential issuer.

Market Motivators

The Open Identity Exchange recognised and sought to explicitly address several motivators when it went about architecting consistent, centrally-governed exchange of digital attributes:

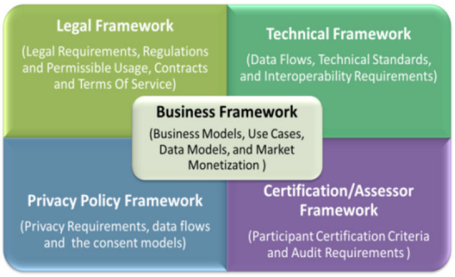
- *User Trust* is the most central determining factor for the adoption and steadily expanded use of new digital services
- *Market Efficiency* (via standard interoperability agreements) to reduce cost and thus help enable and stimulate new services
- *Openness and Transparency* (via standardised agreements) to further improve efficiencies and thus expand digital goods and services markets
- *Credibility and Accountability* for business confidence, user acceptance and legal certainty.

How the AXN Spec was Developed

In January 2012, the OIX community established the *Internet Identity Attribute Exchange Working Group* (AXWG), open to all OIX Members and Contributors as defined in the OIX Member Rules. Commensurate with the broad and ever-growing set of trust requirements being encountered in the identity ecosystem, participation in the AXWG was intense, with representation from:

- *Relying Parties* in government, business and education
- *Identity Providers*: (e.g. Google, AOL, Verizon, AT&T, etc.)
- *Attribute Providers*: (e.g. LexisNexis, Experian, Equifax, PacificEast, Trulioo, etc.)
- *Auditors/Assessors*
- *Standards Organizations*: OIDF, OASIS, Kantara, IDESG, etc.
- *Policy Makers*: regulators, lawyers & legislators
- *End Users*: citizens, constituents, and customers; represented by e.g. the Center for Democracy & Technology
- *Trust Framework Providers*: (e.g. InCommon, FICAM, OIX)
- Government, commercial, and academic entities.

[1] OIX Members: CA Technologies, Equifax, Google, PayPal, Verisign and Verizon.



Working within the OIX Trust Framework Requirements and Guidelines,[2] the AXWG developed first a Charter and then convened five Working Groups covering different framework facets: *Business*, *Legal*, *Technical*, *Privacy Policy* and *Assessment & Certification* (see Appendix C). When communities come to their own AXNs, it is expected that local working groups be convened along similar lines.

Ultimately the AXN Trust Framework Specification was released at the Cloud Identity Summit in July 2013.

[2] http://openidentityexchange.org/wiki/trust-framework-requirements-and-guidelines-v1.

3. The Anatomy of an AXN

The Players

The OIX has laid down the blueprint for standardised Attributes Exchange Networks, which it expects will be implemented on a more or less local level within a spectrum of business environments or "communities of interest". Fundamental to attributes exchange is the philosophy that identity management technologies are always best deployed to fit the business rules and culture of the main layers in any transaction context. When overlaying digital identity and attributes technologies, there is a consistent cast of roles, which are filled by local players in each AXN deployment. They are:

- ***Relying Parties*** (RPs, aka *Service Providers*) are those entities delivering services to specific users (be they individuals or other entities); RPs must have confidence in the identities and/or attributes of their intended users, and must rely upon the various credentials presented to evince those attributes and identities.
- ***Subjects*** are the users of an RP's services, namely customers, employees, trading partners, subscribers and so on.
- ***Attribute Providers*** (APs) are entities acknowledged by the community of interest as being able to verify given attributes as presented by Subjects and which are equipped through the AXN to create conformant attribute credentials according to the rules and agreements of the AXN. Some APs will be sources of authority for certain information; more commonly APs will be brokers of derived attributes.
- ***Identity Providers*** (IdPs) are entities able to authenticate user credentials and to vouch for the names (or pseudonyms or handles) of Subjects, and which are equipped through the AXN or some other compatible Identity and Access Management (IDAM) system to create digital identities that may be used to index user attributes.

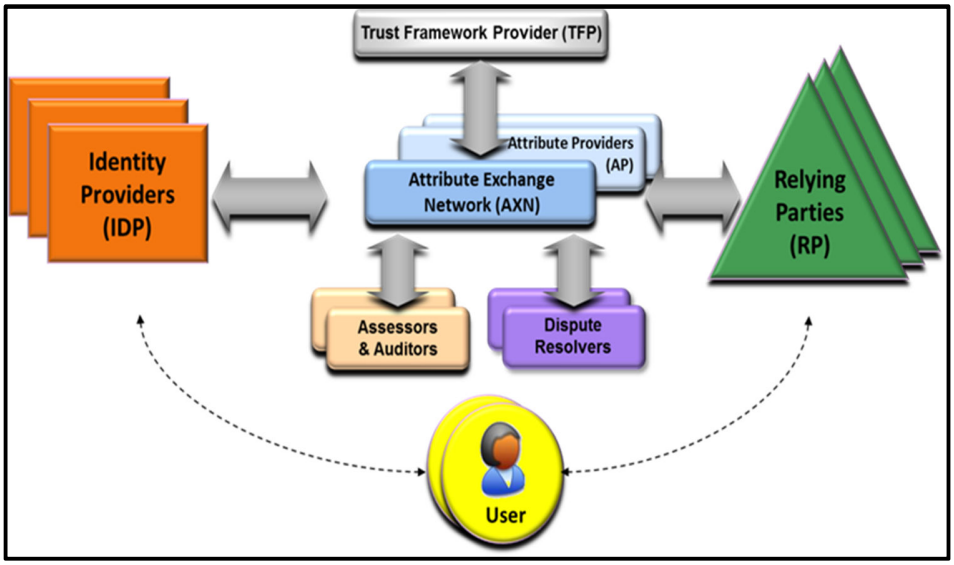


Figure 1 General Attribute Exchange Trust Framework

Critical support players in any AXN include:

- ***Assessors and Auditors*** are necessary in any well-organised identity management system; in an AXN they operate under guidelines that were laid down by the OIX AXF Legal and Assessor/Certification working groups.
- ***Dispute Resolution*** functions established under transparent rules explained to participants when they join the AXN, who work at arm's length from the AXN if and when necessary to help settle disagreements arising.
- ***Trust Framework Providers*** Last but not least, each AXN deployment will be overseen by what OIX terms a "Trust Framework Provider" (TFP). This entity will constitute and coordinate the working groups and the detailed community-specific rule making. In almost all cases, there will be a reasonably obvious candidate organisation to take on this role, for each industry sector or large organisation that decides it is appropriate to interoperate with an AXN.

The "Plays"

Here we briefly overview the types of real-time work flows that the AXN can support in the interests of conveying attribute information about given Subjects amongst participants in an AXN.

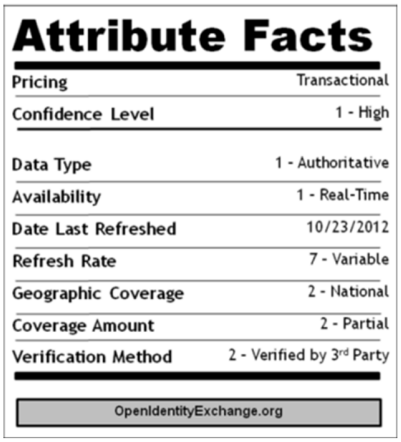
The archetypal attribute exchange play involves a user seeking access to a service, and the Service Provider (i.e. Relying Party) connecting in real time to an Attribute Provider via the AXN in order to obtain – with the user's consent – confirmation of relevant bona fides. This play starts with the user identity being authenticated by an Identity Provider (IdP). In some environments, RPs will be able to select from a choice

of APs. When a number of available APs have signed up to a certain AXN, the AXN will maintain "trust lists" of recognised APs, and can automatically alert RPs of the options that are available to them.

Governance

It has long been recognised by OIX that there can be no trust in any technology or infrastructure without strong and accountable governance. Core to all OIX work is a way of working that combines technology with business, legal and policy considerations, with built-in assessment and certification functions. Likewise, the AXN Trust Framework Specification was developed with governance as a top priority. Any AXN instance recognised by the OIX will have to be constituted with an Assessor / Certification Working Group and will have to incorporate recognised Assessors and Auditors (as shown in the diagram above).

4. The Deep Structure of an Attribute



It could be said that not all attributes were created equal! Consider proof of age. The conventional way to verify that a hotel patron is old enough to drink is to check the date of birth printed on their driver license. And yet few licensing authorities are actually willing to accept legal liability for reliance on this data (for the license is primarily to do with driving, not drinking). Strictly speaking the "source of authority" for age is more usually a bureau of births, deaths & marriages rather than a DMV, but birth certificates are not convenient for routine age checking. In practice, RPs trade off a number of metrics when they decide which attribute providers suit their particular purposes. And so the AXN Trust Framework Specification was put together with careful attention to tools to assist RPs evaluate attributes and APs. The AXN has defined various types of metadata that may be used to reveal the various nuances of attributes that go together to indicate how much confidence may be put into them.

Attribute Metrics

The confidence with which an RP can use an attribute to help make authorization decisions depends on many different factors. Moreover, the factors of interest will vary from one setting to another. It is vital that participants remain free to work out what factors are relevant to them and in what combinations. In general, the RP's confidence will be a function of the type of attribute data, the manner in which the data has been verified by an AP, the rate at which the AP refreshes its attributes, and the time of the refresh. The AXN Trust Framework Specification defines attribute metrics in order to achieve:

1. consistency in the way attributes are referenced
2. standardization and predictability across Attribute Providers
3. a strong and attractive basis for monetization in the AXN.

For details of how attributes are characterised, refer to Appendix A: *AXN Architecture*.

Tools

The AXN Data Dictionary provides several different standardised ways to characterise any given attribute in the system, leaving RPs free to create business rules and real time authorization tests that automatically determine a Subject's bona fides. OIX seeks to facilitate on-going innovation in an emerging attribute market, by fostering a broad array of attributes and APs (fusing traditional approaches and emerging techniques). Starting with standardised attribute data types and metrics (see Appendix A), OIX also anticipates new tools that will help RPs:

- *identify* attributes and APs via easy-to-use intuitive wizards
- compare attribute sources through plain language data sheets akin to "nutrition labels", and
- *select* Attribute Providers when there is a choice on the market.

5. Operating and interoperating an AXN

Different sectors exhibit different risk profiles and business settings, and each has its own rules and regulations for credentialing. Specific arrangements are almost always in place to specify the necessary bona fides for various transactions, and moreover the appropriate authorities to issue them. Attributes exchange will work best when layered on top of existing ways of dealing with parties and doing business, so as to leverage established rules and authority structures.

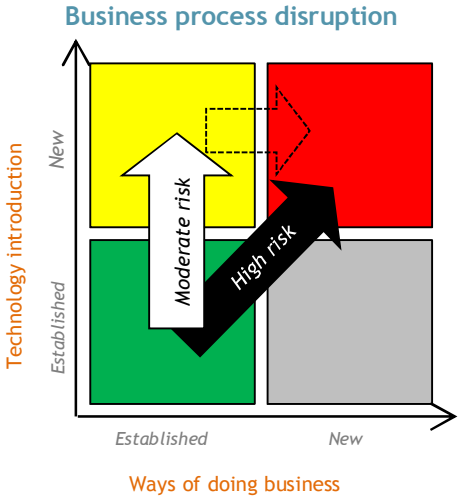


Figure 2: Risks in business transformation

To understand this strategy, recall that in any business transformation project, the risks associated with the introduction of new technologies are generally less serious than the risks that go with changes to business practice (see Figure 3). Despite the competitive threat created by agile new market entrants, most businesses that have successfully adopted e-commerce have done so by first maintaining their tried and proven business practices while phasing in digital technologies, before then proceeding to measured business process re-engineering. Looking at attributes exchange in this light, it will generally be best for organisations to initially preserve their established business rules, automate authorization processes using digital attribute information, and after the technology is bedded down, look to leverage it for a secondary wave of business process reengineering.

Communities of Interest (COIs)

The basic objective of a sector specific AXN is to automate the authorization of transacting parties, using attribute exchange technology to convey machine readable information about what people are allowed to do within the sector. Every COI is different. Each has its own sets of regulations (and laws in some cases), conventions and plain old habits for doing business. And in each sector – be it banking, healthcare, government, retail, property, or the professions – there is typically a standard set of recognised credentials and recognised authorities to issue them. Some of these may be legislated, while others will have evolved naturally across a sector; in any case, all credentials and credentialing rules are subject to continuous change as the world itself is constantly changing.

Working Groups

Following the success of the five WGs that jointly developed the AXN Trust Framework Specification, it is strongly advised that if and when a Community decides to interoperate with an existing AXN or build its own AXN, then it should follow the same program oversight formula. That is, COIs should establish:

- Business WG
- Legal WG
- Technical WG
- Privacy Policy WG and
- Assessor/Certifier WG.

When the COI formally joins to the AXN, participants will have to execute various Operating Agreements with the Trust Framework Provider (see below); the WGs will help ensure that the community's interests are properly represented and realised. Note that the human and financial resource commitments for these activities need not be excessive; these activities can almost always draw on existing expertise and intellectual capital. The sorts of COIs that have an interest in attributes exchange have typically already invested in business analysis, management processes and infrastructure to support sophisticated online transaction systems, and can reuse these efforts in their AXN. However, it is essential that the COI pay close attention to the customisation of the AXN specification to the local business environment, through the suggested WG structures.

Risks

The main risks faced by any community of interest seeking to deploy digital attributes – and the ways in which the AXN model should help manage them – are as follows:

- ***Identification Risk***: Simply put, the risk that identity data collected about a given user is incorrect (or associated with the wrong user), thereby degrading the reliability of the overall identity system. This tends to be the most basic risk and may often be traced to the quality of conventional identity documents (or "feeder credentials") provided by individuals to bootstrap their digital accounts. Correcting for identification risk generally comes down to the diligence of human enrolment processes, although it should be noted that digital identity management systems greatly enhance the detection of fake identities and containment of the adverse consequences, both in respect of time taken to respond, and limiting the reach of identity fraud.
- ***Authenticator Technology Risk***: Identification and attributes are of no value if they are not conveyed accurately to Relying Parties and Service Providers who need to know about them. Authenticator technologies (be they physical tokens or devices, or auxiliary communications channels) can fail in various ways, preventing identification from getting through to those who need it, or allowing identification to be tampered with or counterfeited. The AXN approach provides some protection against technology risk by fostering a wider choice of authenticators.
- ***Privacy Risk***: AXN participants must be alert to privacy management principles, such as *Collection Limitation*, *Use Limitation*, and *Transparency*. It is possible that bringing RPs, APs and IdPs together through an AXN will introduce new PII flows and new aggregations of PII even if it is only in the form of audit logs. If an AXN creates new PII flows and aggregations, then these should be documented and justified in the context of improved identification and attribute verification processes. All new PII collection and usage specific to the AXN should be explained in a Privacy Policy or Data Use Statement available to users of the system.
- ***Data Security Risk***: AXNs, as with all identity management systems, carry particular security risks, as compromise of their data assets can in principle be used to perpetrate fraud, undoing the very benefits they are expected to deliver. AXNs should be implemented with especially high levels of data security. Overall data security risk in AXNs can be reduced compared with conventional IDAM systems thanks to the way they limit information flows to attributes specific to the transaction at hand.
- ***Legal & Regulatory Risk***: The AXN Trust Framework Provider and participants must satisfy themselves that they understand potential liabilities arising from foreseeable system failings, and from the jurisdiction(s) and sector(s) in which they will operate. It is essential that the Community of Interest concerned constitutes a Legal Working Group, which will help

define and analyse risks and compliance obligations specific to their business setting, and the enforceability of the AXN's various legal strategies and contractual mechanisms.

Operating Agreements

An AXN is underpinned by formal contracts executed between framework participants and the trust framework provider (TFP):

- **Identity Service Provider Agreements**: between the TFP and each certified IDP.
- **Relying Party Agreements**: between TFP and each certified RP
- **Attribute Provider Agreements**: between the TFP and each certified AP
- **Assessor & Certifier Agreements**: between the TFP and each recognised assessor and certifier, binding them to use a standard set of OIX endorsed processes, ensuring consistency across all AXNs under the OIX umbrella.
- **General Terms of Service (TOS) Agreements** may be developed as a centrally available resource for the benefit of users in the community that do not otherwise have contracts in place with applicable Aps, IdPs and/or RPs.

During the course of joining a COI to an existing AXN, or establishing a new AXN, the TFP through its Legal Working Group will draw up templates for all these agreements (starting if they like with pro formas developed by the OIX Legal WG).

Accreditation

The governance element of the AXN Trust Framework Specification requires that any new attributes exchange network have an integral accreditation function. As and when attributes exchange takes hold in identity management practices, OIX expects that contestable accreditation options will emerge from the information security audit marketplace. In the initial stages of the development of AXN practices, accreditation will have to be sourced on a bespoke or individual basis; in some cases depending on sectoral and RP specific risk profile and risk appetite, self-accreditation may be acceptable, using the AXN Trust Framework Specification itself as the benchmark. The Community of Interest's AXN legal WG and Trust Framework Provider will have to consider the accreditation options.

6. How to get involved

Selection Criteria

Good candidates for adopting attribute exchange technology include large-scale transaction providers in regulated or relatively high-risk industries where authorization decisions depend on specific bona fides that can be obtained from recognised authorities. In the past, some established businesses and industry groups have tried federated identity but struggled with legal complexities such as new forms of Terms and Conditions. It can be difficult to frame Ts&Cs for general purpose identity provision, but the contractual arrangements for attribute provision are generally simpler, because they tend to conform to conventional business activities. If an existing organisation is already "in the business" of managing professional memberships, issuing defined credentials or vouching for demographic details, then it may well be able to stand up an API to its member database and provide its authority information via OIX protocols.

OIX Resources

The AXN Trust Framework Specification is augmented by a range of presentations and white papers (including this document) at the OIX web site http://openidentityexchange.org.

Implementation Partners

Establishing a new AXN will be a significant undertaking. As emphasised throughout this paper, building and supporting an attribute exchange system is a multidisciplinary exercise and calls for sophisticated project management. Fortunately, the AXN Trust Framework Specification was developed by a broad church of organizations steeped in contemporary identity management; the document reflects the state-of-the-art in digital technologies project management and risk management.

Organisations contemplating their own AXN, or looking to join an existing AXN, may be well served by any one of a number of advisers or systems integrators from within the OIX foundation membership.

A: AXN Architecture

Data Model, Data Types and Metrics

The data model has been designed to provide metadata about attributes to Relying Parties allowing them to calculate levels of confidence, and to extract pricing signals. Each attribute can be characterised by the following metrics, each of which can be assigned various values:

Metric & Possible Values		Definition
Data type	*Authoritative*	Created by source of authority or licensed reseller
	Aggregated	Combination of data from multiple sources
	Direct Captured	Data about the Subject, collected directly
	Self-Asserted	Asserted by the Subject about themselves
	Derived	A value calculated by a proprietary rule set
	N/A	Not applicable
Availability	*Real time*	Average response time less than 5 secs
	Not real time	Average response time greater than 5 secs
Geographic Coverage	*Global*	Data covers multiple countries.
	National	Data covers one country.
	State / Province	Data covers one specific state, province or territory
	N/A	No coverage or otherwise not applicable
Coverage Amount	*Full*	90% or more of the given area, domain or service
	Partial	40-90% or more of the given area, domain or service
	Minimal	40% or less of the given area, domain or service
	N/A	No data coverage
Verification Method	*By issuer*	Verification by the AP
	By 3rd party	Verification by a third party AP
	Out of band	Verification by out of band signal
	Not verified	Not verified
	N/A	Not applicable
Refresh rate	*Real time*	Refreshed/updated immediately, or within 12 hrs
	Daily	Refreshed/updated at least once a day
	Weekly	Refreshed/updated at least once a week
	Monthly	Refreshed/updated at least once a month
	Annually	Refreshed/updated at least once a year
	Never	Never refreshed/updated.
Currency/ Refresh	*<date>*	Actual date value

The data model allows RPs to calculate for example confidence levels as customised functions of Data type, Verification Method, Refresh rate and any other metrics of interest in their particular contexts.

B: Business details: Monetization

Commercial sustainability of Attribute Exchange Networks was a primary consideration of the founding AXN Working Group. A contestable marketplace of profitable commercial service providers is

regarded by all concerned as essential for the long term viability of federated identity. The AXN WG envisioned several different ways for Attribute Providers to make money.

The AXN blueprint can support a number of different monetization models. In general, revenues for AXN services will be generated from customers of RPs paying for services or digital products delivered by those RPs. Prices for APs' services will settle out under free market forces and will naturally be factored as necessary into RP charges. In principle, payment may be effected on a per-transaction, periodic subscription or some other basis. Prices charged by APs are expected to vary according to the data type and quality, market coverage, currency and other factors; in time, APs may bundle their attribute services with other offerings to enhance their commercial attractiveness.

Considerable effort has been put into the AXN architecture to ensure commercial sustainability. OIX envisages several alternative monetization models, including the following archetypes:

The Attribute Exchange Model typically prices APs' fees per transaction, but also allows RPs with high volumes of user access to pay per user per year. This model represents an open online marketplace where IdPs and APs compete for RP business and the user is not charged expressly to participate. The expectation is that RPs will pay less than what they currently pay to validate user attributes; and IDPs and APs will increase their revenue.

The Verified Identities model is a specific case where an IDP takes core attributes (e.g. name, address, age and other demographics) from one or more APs for the purpose of identity proofing and issuance of an identity credential. The attributes themselves are not exposed in this model, and are not discretely priced to the end RP but instead are paid for by the IdP on some negotiated basis that would reflect the quantity and quality of the identities produced. The Verified Identities model can of course be combined with other attribute pricing via the AXN when bundles are made up of identities and other assertions.

C: AX Working Group

The AXN was brought into being by the OIX Attribute Exchange Working Group and five sub-groups:

AX WG Leadership and Charter Members Dave Coxe (ID DataWeb, co-chair) Peter Graham (co-chair) Don Thibeau (OIX, ex officio member) Peter Graham & Dale Rickards (Verizon) Eric Sachs (Google) Dave Coxe (ID/DataWeb)				
Business	**Legal**	**Technical**	**Privacy Policy**	**Assessor / Certification**
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* *Scott Rice* Trulioo *Tanis Jorge* *Stephen Ufford* Individual *Andrew Nash* UnboundID *Trey Drake* *Nicholas Crown*	**Edwards Wildman Palmer LLP** ***Tom Smedinghoff*** LexisNexis *Federico Bucspun* LexisNexis *Katie Ray* ID DataWeb *John Dials* ID DataWeb *Dave Coxe* Accenture *Domenic Dillulo* NIST *Naomi Lefkovitz* Verizon *Dale Rickards*	**Ping Identity** ***Pamela Dingle*** *John Bradley* AOL *George Fletcher Amine Rounak* ID / DataWeb *Chris Donovan* *Ravi Batchu* *David Coxe* PacificEast *Scott Rice* Verizon *Peter Clark*	Verizon *Dale Rickards* *Rich Furr* *Peter Graham* NIST *Naomi Lefkovitz* Privacy Consultant *Debbie Diener* Edwards Wildman Palmer LLP *Tom Smedinghoff* PacificEast *Scott Rice* Accenture *Domenic DiLullo* Individual *Michael Brody* ID / DataWeb *David Coxe* Individual *Nick Kalisperas*	Deloitte *Ray Kimble* *Myisha Frazier-McElveen* eCitizen Foundation *Dan Combs* Electrosoft *Sarbari Gupta* KPMG *Nathan Fault* ID / DataWeb *David Coxe* IDmachines *Sal D'Agostino*

Glossary

AP	Attribute Provider
API	Application Programming Interface
AX	Attribute Exchange
AXWG	Internet Identity Attribute Exchange Working Group
BPR	Business Process Re-engineering
CIO	Chief Information Officer
COI	Community of Interest
DMV	Department of Motor Vehicles
FICAM	Federal Identity, Credential, and Access Management
GPG	Good Practice Guide (of the UK IDAP)
GSA	General Services Administration (US)
ICF	Information Card Foundation
IDAM	Identity and Access Management
IDAP	Identity Assurance Program (UK)
IDESG	Identity Ecosystem Steering Group (of NSTIC)
IDM	Identity Management
IdP	Identity Provider
KBA	Knowledge Based Authentication
LOA	Level of Assurance
NHS	National Health Service (of the UK)
NSTIC	National Strategy for Trusted Identities in Cyberspace (US)
OECD	Organisation for Economic Cooperation and Development
OIDC	Open Identity Connect
OIDF	Open ID Foundation
PDS	Personal Data Store
PII	Personally Identifiable Information
REST	Representational State Transfer [a software development philosophy]
RP	Relying Party
SAML	Security Assertions Markup Language
SP	Service Provider
SOA	Source of Authority
SSO	Single [or Simplified] Sign On

2FA	Two Factor Authentication
TFP	Trust Framework Provider
TFPAP	Trust Framework Provider Adoption Process
TIG	Technical Implementer's Guide
TOS	Terms of Service
UMA	User Manage Access
UX	User Experience
WG	Working Group

References and Further Reading

OIX

http://openidentityexchange.org

AXN Trust Framework Specification

Available from the OIX web site.

Open ID Foundation

http://openid.net/foundation