OPEN IDENTITY EXCHANGE

White Paper

Aligning the Rules and Tools of Digital Identity

Solving Today's Burning Business Problems

Don Thibeau

Open Identity Exchange

Introduction

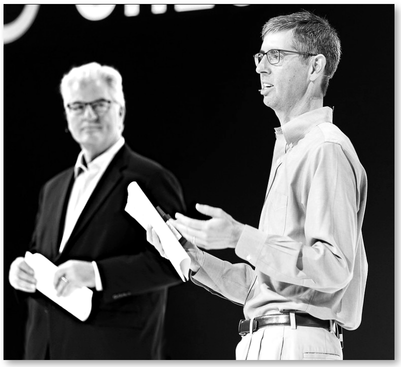
Identity is a wicked problem. Its wickedness lies in part with the MIMO multi-input/multiple output nature of identity. Identity solutions require an alignment of tools and rules.

That alignment is instantiated in tools like open identity technical standards and governance rules in trust frameworks that specify the duties and liabilities of each signatories of these multi party contracts.

The continuity of standards is required to ensure the identity is portable and accessible across the identity framework. But we still have to work out how we share data among Relying Parties, intermediaries, and identity custodians.

It is clear that CCPA-like regulation is coming to all of the U.S. which presents many opportunities for innovation and industry collaboration, for we know that no one company nor one industry can be the focal point of digital identity, a monolithic approach will not work, an equanimous approach will work.

This paper advances the conversation in the current digital identity landscape. It went "live" on a stage in London when Eric Sachs and I described ten years of identity "battles". These are a set of burning business problems facing the internet identity world that no one organization can solve alone.



This paper further marks the beginning of a new approach to solving these problems with initiatives in 2020. I want to thank the organizations I help lead, the OpenID Foundation and the Open Identity Exchange for supporting this effort.

I also want to thank the many contributors, friends, and colleagues who I've nagged, cajoled and abused to make this paper possible, readable and hopefully value adding. Chief among them are Ken Allen, Bill Crean, Pete Graham, Bjorn Hjelm, Alison LeBreton, Mike Leszcz, Nick Mothershaw, Scott Rice, Eric Sachs and Taylor Ongaro.

- Don Thibeau

Don is the Executive Director of the OpenID Foundation, a non-profit international standards development organization of individuals and companies committed to enabling, promoting and protecting OpenID technologies. The Foundation's membership includes leaders from across industry sectors and governments that collaborate on the development, adoption and deployment of open identity standards. Formed in June 2007, the Foundation serves as a public trust organization representing the open community of developers, vendors, and users while providing needed infrastructure and leadership in promoting and supporting expanded adoption of OpenID. Don is also the Co-Chair of the OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) Technical Committee.

Table of Contents

Introduction 2

Executive Summary 4

1. Identity Landscape 4

1.1 Basic Concepts of Modern Identity 5

1.2 Relationship between Users, Identities, Identifiers, and Attributes 6

1.3 Attributes: The Currency of E-Business 7

2. Challenges and Opportunities 8

2.1 Diversity of Views and Priorities 9

2.2 Consumer Consent 10

2.3 Identity Custodians 11

2.4 Continuous Authentication 11

2.5 ZenKey (Project Verify and Mobile Authentication Taskforce) 12

3. Solutions 13

3.1 Open Market Attribute Exchange Trust Framework 14

3.2 OpenID Connect MODRNA Profile 16

3.3 OpenID Connect Financial Grade API (FAPI) Profile 17

3.4 Distributed Ledgers (Blockchains and Hashgraphs) 18

4. Recommendations 19

4.1 Use Open Standards 19

4.2 Collaborate, Don’t Isolate 19

4.3 Build Consumer Consent Supporting Multiple Types of Engagement 20

Executive Summary

In an era governed by digital transactions and data, our methods for managing digital identities, security, and privacy are proving inadequate. At the same time, consumers are looking to do business with companies that have minimal friction as part of their overall service experience, and which provide assurance that consumer's identities and transactions are reliable and safe. Digital identity has matured from a first-in, first-out type of workflow to a multiple-input, multiple-output object-oriented entity, making it more difficult than ever for businesses to know what data to use, how to use it, and when to use it.

To our collective chagrin online "trust" remains elusive in part due to numerous large-scale breaches, cyberattacks, and data-driven scandals. At SWIFT Innotribe@Sibos 2019, Eric Sachs of the Microsoft Identity Team observed:

> *For those of us in the identity community, this is definitely a year of pounding our heads against a brick wall.*[1]

Overall trust in digital ecosystems is diminishing, which overlaps with some digital identity concerns, all relating in some way to the unauthorized release or use of individual identity and information tied to identity, often on a mass scale. Common sense tells us that regulations such as the California Consumer Privacy Act (CCPA) are coming to the entire United States, so the timing is conducive for rethinking how we approach digital identity. The vision is one of competent authority supporting private and public sector businesses and interested parties in building digital identity services, fit for their purposes and in their own environments that are secure, reliable, and easy to use.

As the Internet of Things takes off and cryptocurrencies become widely used, we must also embrace enabling technologies such as distributed ledger technology and peer-to-peer applications developed using open source, standards-driven, transparent, interoperable digital identity.

To promote this digital identity utility, we make the following observations and recommendations:

- Consumer choice is a key driver for digital identity innovation.
- Implementation efforts will be in vain unless standards are adhered to.
- Build upon a *competent authority* paradigm for the maintenance of digital identity.
- Acknowledge that no one company can do it all, no one industry segment can be the center of the identity universe, and everyone is a participant in the collective digital identity commons.
- Promote consumer engagement with *continuous authentication* and *portable consent*.
- Attribute Exchange Network (AXNs) and registries are crucial.

1. Identity Landscape

Buck Rogers' future is now. Our world is characterized by highly distributed computing systems operating with decentralized governance and cross-border corroboration handling billions of identity-driven interactions and user verifications every day. We see this play out across business sectors in the disruption of global banking networks via open banking and changes triggered through privacy regulations such as the General Data Protection Regulation (GDPR). As countries and U.S. states pass

[1] Eric Sachs, Partner Director of PM at Microsoft, Sibos (Innotribe): Privacy - Fintech vs consumer login (26 Sept 2019).

new consumer privacy and data collection regulations, companies must view digital identity through a prism of *direct* and *indirect* (or *inferred*) data attributes. As always, innovation is key to responding to disruption and to creating additional disruption opportunities.

Overall, we find that the finance space has had success with ongoing digital identity innovations to offer more payment choices to users while improving security and usability and leveraging global standards. Unfortunately, the same cannot be said of the bespoke consumer login space, in which there are few choices for interaction (mostly passwords) and few examples of improving security, much less usability. It has myriad standards, but very few have found global adoption.[2]

That is why carriers and financial institutions must take the lead. They are exceptionally well positioned to close the gaps in digital identity.

First, institutions perform many digital identity functions as a normal course of business. They already store and verify user information. Their operations span multiple jurisdictions. They have a proven ability to create new systems and standards. In developed economies, their coverage of people, legal entities, and assets is nearly universal.

Second, they are mature. Carriers and financial institutions' operations and use of customer data are strictly regulated. They are the intermediary of record in many transactions. Consumers trust financial institutions with their information and assets more than they do many other custodians. Robust, inclusive, and responsible digital identity systems accommodating complex roles and transactions can increase access to finance, health care, education, and other critical services and benefits.

Identification systems are also key to improving efficiency and enabling innovation for public- and private-sector services, such as greater efficiency in the delivery of social safety nets and the facilitation of digital economy development. Yet many operators, especially incumbents, struggle to meet these expectations, which has historically been due to a lack of consumer trust in sharing private information online and is currently due to the increasingly complex technical requirements and challenges presented by legacy IT systems.

1.1 Basic Concepts of Modern Identity

An identity comprises many different pieces of information (also called *attributes*). The more attributes that can be leveraged for a given identity, the greater the checks and assurances that can be made about the identity. For example, the state can issue someone a unique number. By itself, the number tells us almost nothing. Combined with the person's name and date of birth, it tells a bit more. Add a photo, mobile number, residential address, school records, and work history, and suddenly it tells a lot about a person.

People are not the only ones who have identities. So do legal entities (such as corporations and trusts) and assets (property). The attributes that go into an identity help others decide whether to engage in a transaction with it—for example, whether to accept its vote, open a savings account for it, or sell it a bottle of wine. The same is true for legal entities and assets. Certain identity attributes help others decide whether to do business with the owner, representative, or custodian.

[2] Eric Sachs, Partner Director of PM at Microsoft, Sibos (Innotribe): Privacy - Fintech vs consumer login (26 Sept 2019).

Assurance, which refers to the degree of certainty that the identity is real and belongs to the person using, it is a key factor in identity transactions. Some transactions, such as registering on a news site or paying a parking ticket, might not be worth the work it takes to authenticate an identity to a high degree of certainty. The opposite is true for transactions like using an online brokerage account or receiving certain government services. Those must be *high-assurance transactions*.

Identity transactions tend to form networks based on the type of identity. For example, government identity systems and employee management systems form around individuals. Business registries and industry identifier systems form around legal entities. Asset registries form around . . . you get the idea.

All identity systems, however, have a few characteristics in common:

- They all have users who get an identity in the system so they can carry out transactions.
- They all have Identity Providers, who store user attributes, ensure they are genuine, and complete transactions on the users' behalf.
- They all have Relying Parties (RPs), who serve users after Identity Providers vouch for them.
- They all have a governance body that oversees the system and makes the rules.
- They are all based on a platform that completes the transactions by providing all parties with reliable evidence.

So far, none of this is novel. It is the same system that people have used throughout history. Someone arrives at an employment office bearing a letter of introduction; he or she is a user. The letter is from someone who vouches for the user; the author is an Identity Provider. The one to whom the letter is addressed is the Relying Party. The Relying Party decides whether to accept the letter's claims based on their own judgment and what they know about the Identity Provider.

A digital identity system follows this same process, only electronically. Using a digital identity system has several advantages:

- It is easier to share among all parties of a transaction.
- It can include much more dense information than a collection of physical documents can.
- With the proper technology, it can give users much more control over how their information is stored and used.

1.2 Relationship between Users, Identities, Identifiers, and Attributes

The ISO standard IEC 24760-1 defines identity as a "set of attributes related to an entity"[3]; within the context of the digital world, that is information on or about an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. There is a 1:n relationship between a user and a user identity, making digital identity management progressively complex.

In the science of identity management, something outside a system that needs to be identified in the system is referred to as an *entity*; an entity is sometimes called a *user*. A user is not necessarily a person; it could also be an application or a device (e.g., thing). The entity is uniquely represented by an identity

[3] IT Security and Privacy – A framework for identity management, ISO/IEC 24760-1:2019.

in the system, while the identity is dependent on the role of the entity in the system (i.e., which kind of service is used for which purpose), as illustrated in Figure 1.

That leads us to exclaim, “Aye, there’s the rub,” as an individual can have several user identities—for example, one user identity that represents the professional role of the (human) user, and another that represents aspects of their private life.

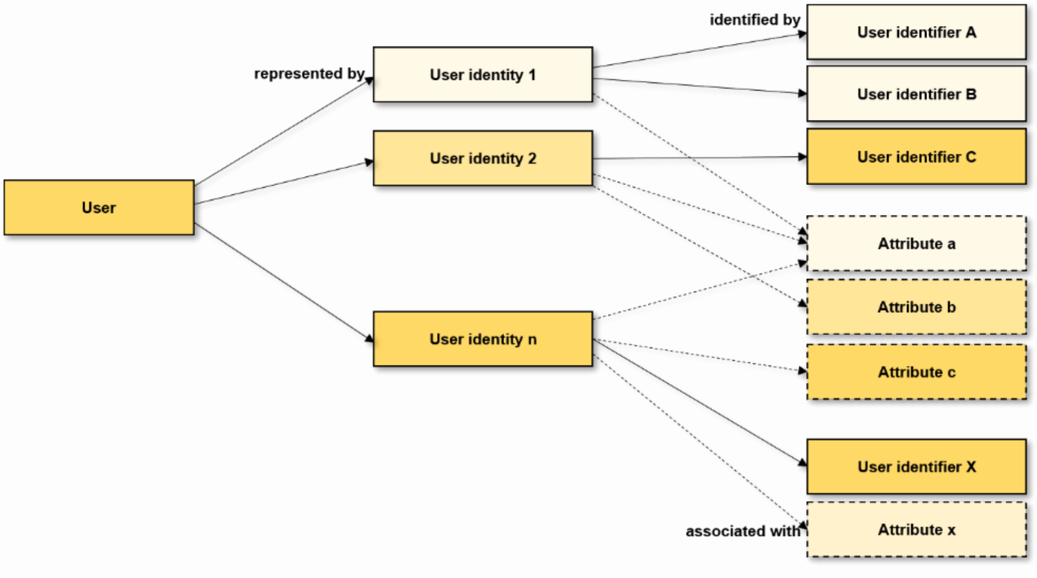


Figure 1. Relation between users, identities, identifiers, and attributes[4]

1.3 Attributes: The Currency of E-Business

Attributes are the currency of transactional business; they enable a party to verify that a counterparty is authorized to deal in the transaction. For example:

- A merchant needs to know a shopper’s credit card number (and, depending on the goods involved, perhaps the billing address and the customer’s age).
- A pharmacist does not 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 a minor.
- A consultative health chat room may desire that anonymous users meet criteria for participation.
- A drug company running a clinical study must be sure of participating patients’ and investigators’ trial identifiers, while keeping their identities confidential.

Despite the centrality of attributes in routine business, until recently there was no uniform method for exchanging and acting on attribute information digitally.[5]

[4] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; study on user centric identifiers and authentication (Release 16); (09-2018), 3GPP TR 22.904 V16.

[5] Attribute Exchange Networks: New Infrastructure for Digital Business (October 2013). OIX | Steve Wilson, Lockstep Consulting.

A digital identity is a version, or facet, of a person's social identity. We can say that *digital identity* is the sum of all digitally available data regarding an individual, regardless of its degree of validity, its form, or its accessibility, comprised of *direct* and *inferred* (or *indirect*) data, as illustrated in Figure 2.

Digital identity is now often used in ways that require data about people stored in computer systems to be linked to their civil (national) identities. The use of digital identities is now so widespread that many discussions refer to digital identity as the entire collection of information generated by a person's online activity. This includes usernames and passwords, online search activities, date of birth, social security number, and purchase history, and *attribute facts* among a multitude of additionally available elements.

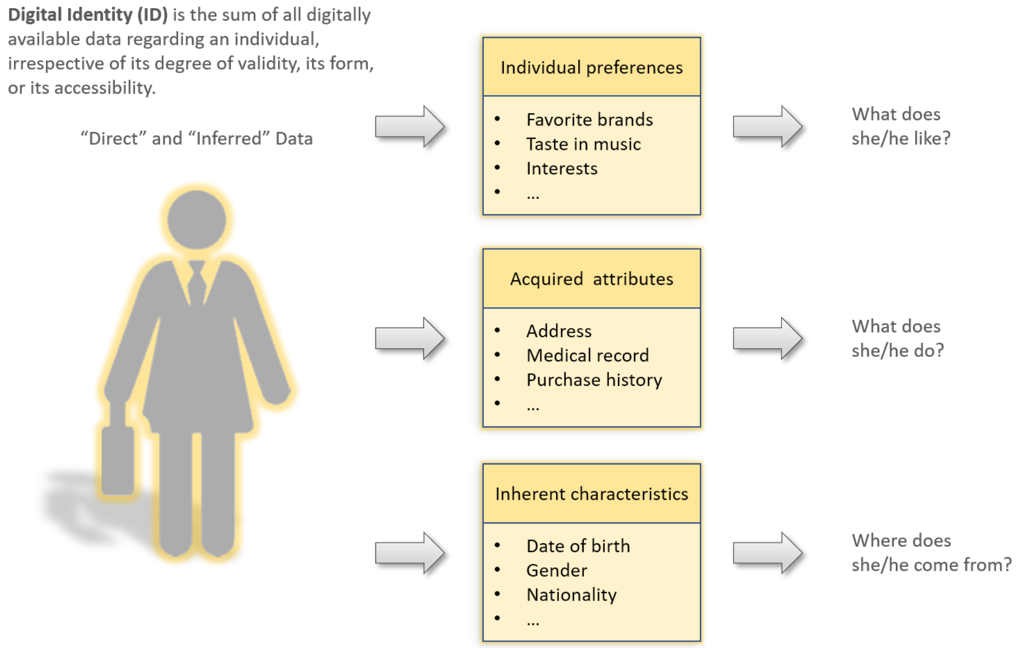


Figure 2. Digital identity elements (preferences, attributes, characteristics)

2. Challenges and Opportunities

Customer identification is important because it is at the center of many financial services processes. Institutions need it to comply with regulations, assess risk for insurance and credit, and provide a tailored customer experience. Detail and accuracy are critical. Digital identity promises to improve these processes while removing inefficiencies. But the relevance of digital identity extends beyond financial services.

Think about public services that require proof of identity, such as social security, unemployment insurance, education, healthcare, and polling. Proof of identity is also necessary in many aspects of private commerce, such as buying alcohol, renting an apartment, and purchasing a car.

Bill Crean, Product Manager for Identity and Authentication at Verizon, commented:

> *When we get digital identity authentication right—secure, reliable, and easy to use across the globe—and it removes friction and helps to prevent fraud, then we can ask what can businesses,*

> *carriers, and the entire ecosystem do with that? The answer is that we can do anything we want more efficiently and more safely.*[6]

And the need for a digital solution is becoming urgent. Transactions are growing in volume and complexity. Customers increasingly expect seamless, omnichannel service, and they will take their business elsewhere if they do not receive it. Regulators, for their part, are demanding greater insight into transactions. They will hold firms responsible if identity information is missing or inaccurate.

2.1 Diversity of Views and Priorities

Adding to the confusion in the digital identity landscape is a diversity of views and competing arguments for how best to implement and manage the privacy and security of digital identity. There is the "pro-business" wing, which tries to meet the needs of RPs to access information and to manage business processes and prevent fraud with stringent controls; and there is the "pro-consumer" wing, which wants to give consumers complete and total control over their information. Although these two wings appear to have organized at opposite ends of the spectrum, this is a false dichotomy.

Privacy and data protection regimes establish *predictable rights* and *obligations* regarding the treatment of individual data and Personal Identity Information (PII) that are an important part of establishing trust in digital systems—trust that encourages use. Privacy is not linear; it's circular. Consumers want control over their identity, how it is used, and how they are communicated with; at the same time, they often do not understand what the consent they are granting actually means, and they do not have control over the level or frequency of consent requests occurring related to their identity. But consumers also want to interact with businesses in ways that are not limited to showing up in person with cash and walking out with physical goods.[7]

The interconnected world relies heavily on card-not-present and consumer-not-present commerce. As a result, both consumers and businesses must work together to enable commerce while maximizing privacy and minimizing fraud. Consumers need businesses to provide services in exchange for money. Businesses need consumers to provide revenue in exchange for products and services. A data breach is the business's failure to secure consumer identity information. Fraud is proof that the consumer does not have real control over their identity information.

This interconnectedness requires acknowledgement of a codependence between businesses and consumers that cannot exist at either the *self-sovereign* or *consumer-data-Wild-West* ends of the spectrum. The unyielding self-sovereign identity approach does not properly account for consumers' dependency on and desire for goods and services for which they do not pay cash in person.

To solve this problem, the identity community has tried to connect identity silos in various federated models. However, these have produced inadvertent side effects such as concentrating control around a small number of providers, increasing data leakage through inadvertent sharing, and raising privacy concerns, all while not actually giving the individual real control. At the same time, there is a growing economic inefficiency when organizations globally must collect, store, and protect the same sort of personal data in their own silos. It is reaching a tipping point.

[6] OIX Interview – Bill Crean, Product Manager - Identity and Authentication at Verizon (6 May 2019).
[7] The Shared Signals Model – Distribution of Significant Account Events (20 September 2013). OIX | Andrew Nash, Confyrm Inc.

2.2 Consumer Consent

"Consumer consent is still a dysfunctional patchwork that shows no signs of real improvement."[8] Individual U.S. states have conflicting regulations, and enactment of the CCPA may ultimately force the whole U.S. to adopt GDPR-style laws. Prudent, responsive organizations should see any incoming regulation not as a threat to their business model, but as an opportunity to develop innovations that can be key competitive differentiators.

Consumer's *authorization of consent* is one of the greatest difficulties in complex transactions, because all parties to the transaction—the Relying Party, the Attribute Provider, and possibly an Exchange—have differing legal requirements, regulatory restrictions, and expectations for release of information. The situation quickly becomes an interoperability ordeal driven by outdated notice and consent laws. During interview and analysis for this paper, Ken Allen, Equifax Global SVP Identity, Fraud, and Compliance, observed:

> *The challenge is how much truly overt consent is needed versus overt awareness to an End User—or to a business that's using consent on behalf of the User.*[9]

In the same discussion, Bill Crean, Product Manager of Identity and Authentication at Verizon, said:

> *Identity Providers across industries are looking for more opportunities to collect direct consent—to have a more direct relationship with those subscribers. Speaking generally, whatever we can do to have a direct relationship to really know that they (subscribers) are opted in and not opted out, that's going to make everything work more efficiently. It's really about empowerment and transparency for the customer, and everything else is around that.*[10]

Original OIX Telecom Data Working Group (TDWG) Co-Chair PacificEast's Scott Rice added:

> *Consumer consent should be a critical part of the identity management infrastructure, because almost everything that happens post-authentication is focused on what that authenticated user wants to allow. We're getting so good about authentication, but that last bit of managing and tracking consent is frankly still in the Dark Ages of notice and consent laws. We're really focused on high-tech locks, and that's a great first step; but once the consumer is inside, what happens after that is little better than signing a sticky note that you immediately put in your drawer and no one ever looks at again. Consent can't be binary or Boolean. It needs to be within a context that the consumer can quickly but clearly understand, not just a checkbox that adheres to the letter of privacy laws but doesn't mean anything because the consumer has no idea what they're actually consenting to. Existing notice and consent rules require overt consent. There is no construct for overt awareness in the current consent systems. A need clearly exists for a consent inter-exchange standard that disintermediates the consent management needs of Identity Providers and Relying Parties, with tools built to assist human users.*[11]

[8] OIX Interview – Peter Graham, PSG Solutions (24 April 2019).

[9] OIX Interview – Ken Allen, Equifax Global SVP Identity, Fraud and Compliance, and Alison LeBreton, Equifax VP of Communications & Digital Media (29 April 2019).

[10] OIX Interview – Bill Crean, Product Manager - Identity and Authentication at Verizon (6 May 2019).

[11] OIX Interview – Scott G R Rice, PacificEast Research (9 September 2019).

The challenges and burdens on the consumer to maintain bespoke authorization of consent is an area in which distributed ledger technology (i.e., blockchains and hashgraphs) bring new efficiencies and opportunities for enabling and supporting a range of consumer engagement. Similar to other digital identity initiatives using OpenID Connect the AuthorizeConsent.org Registry is a decentralized portable consent management utility deployed on immutable distributed ledgers supporting Enterprise (B2B, B2C) and Peer-to-Peer (P2P) applications and services.

2.3 Identity Custodians

From Eric Sach's talk at Innotribe@Sibos:

> *One model the identity community has experimented with is to keep the concept of Identity Providers (just as credit cards still rely on banks), but to add a third party that helps users manage their consumer internet accounts. Most of that experimentation is as an extension to password safes (i.e., password managers). Some of them are experimenting with acting as a personal Identity Custodian instead of just a Password Manager, where they remember which Identity Provider we consented to use to register for a specific website if we used such a provider instead of a password. If we return to that website or mobile app in the future, instead of seeing a login page, the Identity Custodian already has our previous consent to immediately tell the app who our Identity Provider is, and the website and Identity Provider can then immediately allow sign-in.*[12]

One of the hopes is that browsers and operating systems will allow users to install these Identity Custodians just as they install Password Managers and will allow them to participate in the login flow. Vendors of these custodians could then compete on the balancing of the privacy, usability, and security they provide for consumer logins instead competition in that space for ad networks spilling over into consumer logins.

2.4 Continuous Authentication

There are three main characteristics of secure authentication:

- **Pervasive** – Ensures secure access across the network for all users, applications, and devices (both personal and corporate).
- **Connected** – Information needed for protecting critical assets can be shared across the security ecosystem.
- **Continuous** – Data is collected, analyzed, and acted upon constantly, not just occasionally.

Continuous Authentication (CA) constantly measures the probability of a particular user being who they claim to be, thus authenticating the user not just once but continuously, for the duration of the session. The main idea of continuous authentication is to deliver smart and secure identity verification without interrupting the workflow.

With continuous authentication, instead of a user being either logged in or out, an application continually computes an *authentication score* which measures how certain it is that the account owner is the one using the device. For the sake of simplicity, imagine this score as a number between zero (not

[12] Eric Sachs, Partner Director of PM at Microsoft, Sibos (Innotribe): Privacy - Fintech vs consumer login (26 Sept 2019).

authenticated) and 100 (completely authenticated). If we are not confident enough to warrant, for example, a banking transaction, we can prompt the user to input more information (e.g., password, card, fingerprint). If we detect an action that indicates that the user has changed, we can also decrease this score, essentially making an explicit log-out obsolete.

Another key advantage of continuous authentication is that companies can assign action constraints to each user based on tolerable risk or context. These constraints can consist of a minimum confidence score (derived from the tolerable risk) and other factors such as location of the user, whether other people are present, or even the time of day. This can minimize the exposure of the most sensitive credentials and relieve the stress on the users because they do not need to manage many complex passwords. We find a variety of technologies already exist to support continuous authentication, including Face ID and smartphone fingerprint readers.

Although biometrics are easy to use and seem like a perfect replacement for passwords, they have their own set of drawbacks, which means passwords will still be needed in a world with CA—especially to secure high-risk operations. Biometrics cannot replace passwords entirely because biometric information is immutable: we can't change our fingerprint or behavior, and once it has been stolen, there is no way to reset. However, biometrics are still a valuable supplement to other authentication technologies.

2.5 ZenKey (Project Verify and Mobile Authentication Taskforce)

Significant participants gaining traction in the identity ecosystem are mobile network operator (MNO) services. MNOs provide valuable attributes and services for businesses looking to improve their verification processes. With an estimated 4.8 billion mobile devices worldwide, MNOs have equally enormous potential for helping resolve identity verification challenges.[13]

Accessing MNO data and running effective checks against that data offers another set of attributes that can accelerate the approval process or uncover fraudulent activity. While the availability of these types of MNO data is new or imminent, the ability to analyze and integrate the information is a harbinger of whole new levels of business intelligence. Since these data attributes can be verified directly by MNOs, the strength of authentication and security improves while the risk of fraud significantly decreases with unified and interoperating telecom and non-telecom services.

Keeping data attributes separate also provides individuals with privacy protections. In an era of massive data breaches, having all of a user’s data in one place is an immense risk. Do we want—or need—our credit information and driver’s license information to be aggregated? While MNO data offers many benefits, it is no panacea for identity issues. It can be, however, a valuable set of attributes that contributes to building greater trust in verification and authentication processes.

Fortunately, telecom carriers such as banks and government regulators are slowly pivoting from viewing themselves as the center of their own digital identity universe to recognizing their participation as a crucial constituent of a rapidly evolving decentralized global ecosystem that fundamentally relies on trustworthy identity to operate. Carriers and financial institutions also understand the vital role of government in the context of a collaboration for *governance* partnerships and are in a respected position to provide digital identity gatekeeper stewardship.

[13] Data attributes as digital identity currency (26 February 2018). Marie Austenaa, VP and Head of Identity, GSMA.

Paving the way is the ZenKey collaboration, a result of the Mobile Authentication Task Force formed by the four major U.S. carriers: AT&T, Sprint, T-Mobile, and Verizon. ZenKey, which was introduced in early 2018 under the name Project Verify, is a standalone company focused on evolving authentication and verification capabilities. The ZenKey concept is headed in the right direction for telecom-based digital identity. With ZenKey, the intent is to have everyone use the same door for telecom-based digital identity, whether a Relying Party or consumer of a specific attribute. Unsurprisingly, this new verification system puts carriers at the center, using information only they could possess to authenticate users.

Beyond the sheer number of users, there are numerous data attributes that are unique to MNO providers. These point to a future that offers a richer, more secure user experience with improved customer onboarding processes and risk mitigation for businesses.

Observing the evolution of ZenKey, we are finding active engagement and progressive initiatives; however, the MNOs vary in their approaches, information blocking is inhibiting progress, and the scope of participation is impacting transparency and creating silos.

In an interview, original OIX Telecom Data Working Group (TDWG) Co-Chair PacificEast's Scott Rice said:

> *ZenKey mitigates and partially eliminates silos within carriers by presenting uniform standards across the major carriers. In that process, however, it has created a larger silo, isolating itself from other parts of the identity ecosystem and ecosystem partners by requiring Relying Parties to add ZenKey participants as additional service providers. This is the primary problem with ZenKey, because it inserts an additional layer of closed system paths for Relying Parties. ZenKey can offer identity verification services, but only operates within its closed system, missing the mark for an open, standards-based platform.*[14]

The National Institute of Standards and Technology (NIST) recommended the deprecation of SMS one-time password (OTP) authentication as a second factor for strong authentication as far back as 2016, but the method is still widely used today.[15] An area Relying Parties can improve their processes is to take advantage of ZenKey and similar digital identity initiatives to augment and replace the use of SMS OTP communications.

3. Solutions

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. Fundamental to digital identity Attribute Exchanges (AXs) 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.[16] Systems that build upon open identity standards have the opportunity to leverage the latest federated identity protocols and ensure all necessary business, legal, technological, privacy policy, and assurance arrangements conform with complex legal and compliance requirements.

[14] OIX Interview – Scott G R Rice, PacificEast Research (9 September 2019).

[15] NIST Special Publication 800-63 Revision 3 URL: pages.nist.gov/800-63-3/sp800-63-3.html

[16] An Open Market Solution for Online Identity Assurance, OpenID Foundation (March 2010). OIDF | Don Thibeau, Tony Nadalin, Mary Rundle, Drummond Reed, Eve Maler.

An example of community-built standards driving digital identity adoption is the OpenID Financial Grade API (FAPI), which brings interoperable digital identity capabilities to the financial services exchanges. Carriers use the OpenID Connect Mobile Operator Discovery, Registration, & Authentication (MODRNA) profile that provides for the specific needs of mobile networks and devices.

3.1 Open Market Attribute Exchange Trust Framework

The Open Market Attribute Exchange (AX) Trust Framework is a community-defined, standards-based approach to managing the full scope of digital identity exchange services with foundations, supported by deep cross-industry analysis and cooperative development, as illustrated in Figure 3.

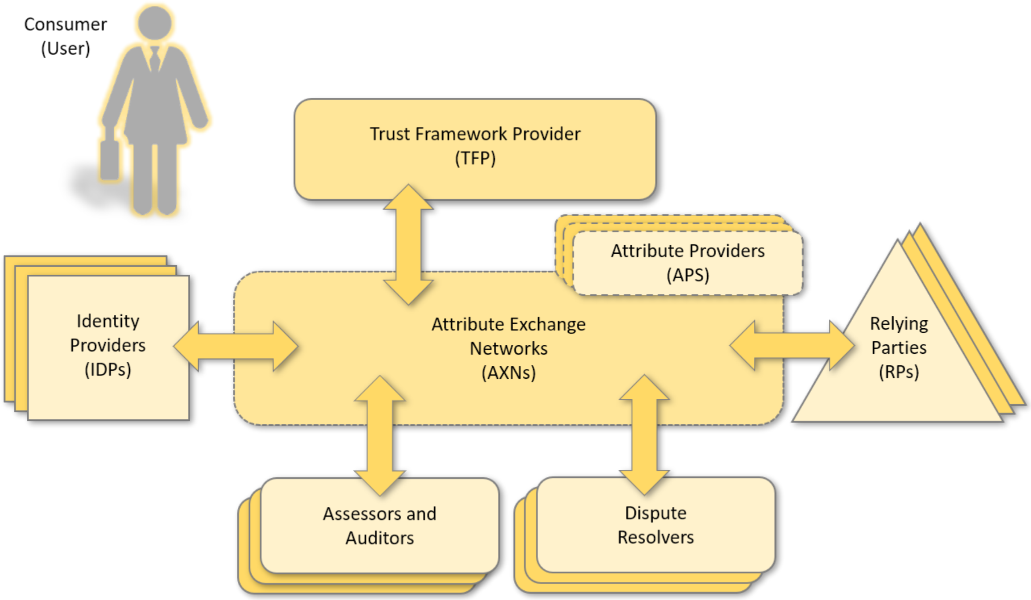

Consumer (User)
Trust Framework Provider (TFP)
Attribute Providers (APS)
Identity Providers (IDPs)
Attribute Exchange Networks (AXNs)
Relying Parties (RPs)
Assessors and Auditors
Dispute Resolvers

Figure 3. Identity attribute exchange ecosystem[17]

Control and privacy are a fundamental aspect of sharing identity data. The Open Identity Exchange (OIX) recognized and sought to explicitly address several motivators when it architected a standard, centrally governed exchange of digital attributes:

- **User Trust** – The determinant for the adoption and expanding use of new digital services.
- **Market Efficiency** (via standard interoperability agreements) – Reduces cost and thus enables and stimulates new services.
- **Openness and Transparency** (via standardized agreements) – Further improves efficiencies and thus expands digital goods and services markets.
- **Credibility and Accountability** – Yields business confidence, user acceptance, and legal certainty.

In an AX, each attribute can be characterized by the various metrics, each of which can be assigned various values, as described in Table 1. This model for standardized AX networks can be implemented across a spectrum of business environments. The data model allows RPs to calculate, for example,

[17] Open Identity Exchange Attribute Exchange Trust Framework Specification v 1.0 (2 July 2013).

confidence levels as customized functions of data type, verification method, refresh rate, and any other metric of interest in their particular contexts, as in the examples depicted in Figures 4 and 5.

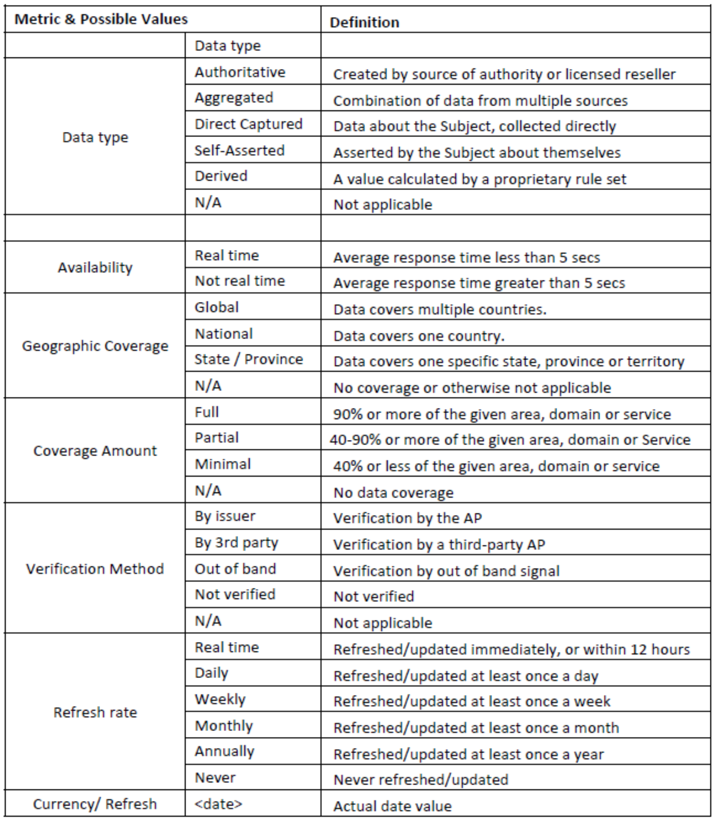
It is critical that the technical and business entities that establish a trusted information exchange model allow competitors to share account information assured that:

- submissions will pose no competitive threat;
- no attribution will be made to an originating source when anonymous submission is required;
- account identifiers within the namespace of the originator will not be shared unless explicitly requested and agreed to;
- policy controls will support configuration of appropriate signal delivery; and
- information will be delivered in a timely fashion.

Efficient, automated AX brings:

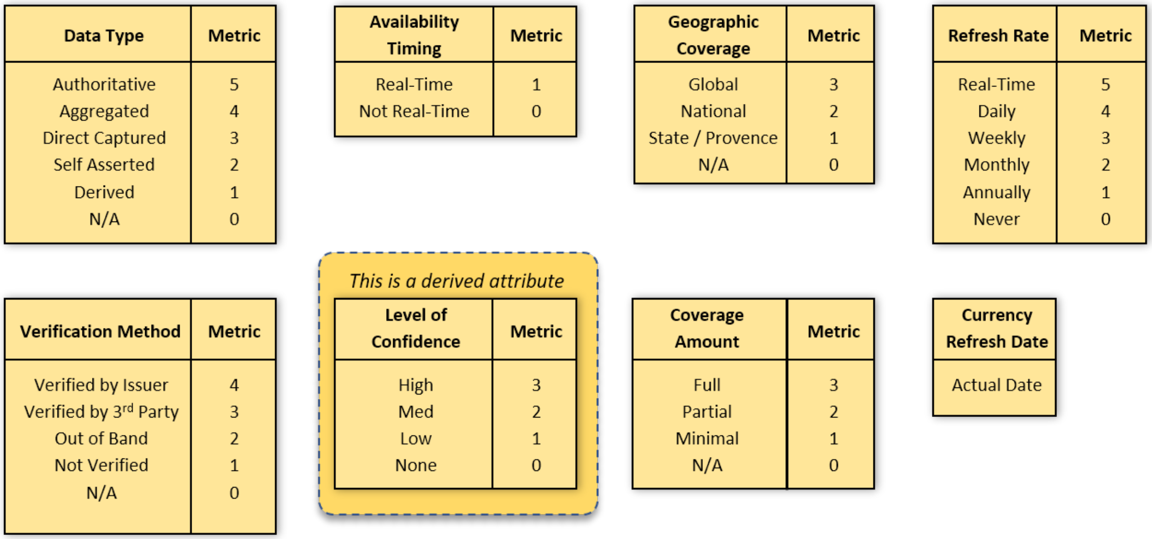
- enhanced privacy as a result of disclosure of only germane personal information;
- simpler liability arrangements and lower legal costs, because it is more straightforward to vouch for concrete attributes than abstract identity; and
- smoother deployment of large digital projects through better preservation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

Table 1. AX attributes[18]



Metric & Possible Values		Definition
	Data type	
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 hours
	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

[18] Open Identity Exchange Attribute Exchange Trust Framework Specification v 1.0 (2 July 2013).



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

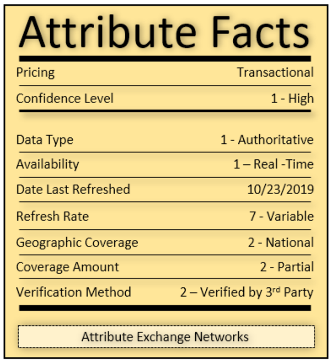
Coverage Amount	Metric
Full	3
Partial	2
Minimal	1
N/A	0

Currency Refresh Date
Actual Date

LOC (Level of Confidence) = fcn (Data Type, Verification Method, Refresh Rate, Currency)

Pricing = fcn (LOC, Coverage, Attribute Type)

Figure 4. Data model and attribute metrics[19]



Attribute Facts

Pricing	Transactional
Confidence Level	1 - High
Data Type	1 - Authoritative
Availability	1 – Real -Time
Date Last Refreshed	10/23/2019
Refresh Rate	7 - Variable
Geographic Coverage	2 - National
Coverage Amount	2 - Partial
Verification Method	2 – Verified by 3rd Party

Attribute Exchange Networks

Figure 5. Attribute facts[20]

3.2 OpenID Connect MODRNA Profile

Established in 2013, the OpenID MODRNA Working Group developed a profile of OpenID Connect, MODRNA, for use by MNOs providing identity services to Relying Parties (RPs), for RPs consuming those services, and for any other party wishing to be interoperable with the profile. MNOs increasingly want to become Identity Providers, leveraging their reach and specific technical capabilities to partners. The MODRNA profile of OpenID Connect is tailored to the specific needs of mobile networks and devices enabling interoperable usage of operator digital identity services.

[19] Open Identity Exchange Attribute Exchange Trust Framework Specification v 1.0 (2 July 2013).

[20] Open Identity Exchange Attribute Exchange Trust Framework Specification v 1.0 (2 July 2013).

Reaching all mobile users in a certain market requires a RP to connect to all its mobile operators. The MODRNA profile provides OpenID Connect mechanisms that enable an RP to get approved for the digital identity service once and connect at runtime to any relevant MNO without having to manually register at each one. As service providers may have different requirements regarding a specific authentication transaction, the profile also defines a set of recommended authentication policies that service providers can choose from. MODRNA has been set up in cooperation with the GSMA in order to support GSMA's Mobile Connect.[21]

3.3 OpenID Connect Financial Grade API (FAPI) Profile

Building on the wide international adoption of OpenID Connect, the Financial Grade API Working Group (FAPI WG) supports a fintech bridge through open standards. The FAPI WG provides JSON data schemas, security, and privacy recommendations and protocols to enable applications to utilize the data stored in the financial account, enable applications to interact with the financial account, and enable users to control the security and privacy settings of the account.

In many cases, fintech services, such as aggregation services, which compile information from databases with the intent of preparing combined datasets use screen scraping and store user passwords. This model is both brittle and insecure. To cope with the brittleness, these services should use an API model with structured data; to cope with insecurity, they should utilize a token model such as OAuth [RFC6749, RFC6750].[22]

The effort to create a more open financial services ecosystem is fostering competition among industry players of all sizes and enabling more innovation in consumer financial products. OpenID Connect FAPI represents the latest thinking in the financial API space, bringing benefits to both the industry and consumers and supporting a number of innovative approaches using a REST/JSON model protected by OAuth.[23]

- **Tailored Risk Profiles** – Financial institutions create a risk profile from a combination of the information they collect about a customer and predictive algorithms. In the future, institutions might make use of the attributes already in the user's digital profile, along with a range of other attributes the user might choose to provide. With more and higher-quality information becoming available, firms could create custom risk and credit products for their customers.
- **International Resettlement** – Anyone trying to open an account without proof of identity is out of luck. If they can establish identity but not financial history, the financial institution might have to move forward anyway if it wants the business. But this "blank slate" situation could be avoided if users bring along a digital identity. Anywhere in the world, users could access financial and other services on the strength of attestations and attributes collected by previous institutions. Each new institution becomes another Identity Provider, further strengthening the user's digital credentials.
- **Digital Tax Filing** – Currently, individuals and businesses alike must gather information from multiple sources—financial institutions, employers, schools, etc.—before they can file their taxes. But digital identity might persuade governments to accept filings from taxpayers' designated financial institutions instead. Firms could use their complete knowledge of

[21] Quoted directly from MODRNA Documentation (www.openid.net/wg/mobile).
[22] The OAuth 2.0 Authorization Framework (tools.ietf.org/html/rfc6749?).
[23] Quoted directly from FAPI Documentation (www.openid.net/wg/fapi).

customers' financial holdings, assets, income, and personal circumstances to automatically complete returns.

- **Determining Total Risk Exposure** – Due to complicated ownership structures and the amount of work due diligence requires, legal entities often find it difficult to determine their total risk exposure in a transaction. Digital identity could provide a consolidated view of each party in a transaction, allowing companies to answer their own questions about risk much faster and at a much lower cost.
- **Identifying Transaction Counterparties** – Identifying all the participants in a brokered transaction can be an onerous task. But with digital identity, legal entities could ask to investigate the consolidated identity of a third party and the ownership history of whatever asset is involved. Knowing more about the direct customer and the end customer would lead to a more informed decision about completing the transaction.
- **Linking Individual and Corporate Identities** – Companies are not necessarily linked to all the people affiliated with them. If the identity attributes for both individuals and legal entities were digitally collected, stored, and transferred in a standard way, financial institutions could get reliable insight into their relationships. The accurate, up-to-date information would comply with KYC regulations, as well as serve many other purposes.[24]

3.4 Distributed Ledgers (Blockchains and Hashgraphs)

Distributed ledgers deserve a significant mention as a proven approach for trustworthy identity infrastructure. Blockchain is an accepted technology that records transactions in chronological order in a decentralized ledger, which is hosted on servers, or "nodes," across a peer-to-peer infrastructure. As one pundit said:

> *Picture a spreadsheet that is duplicated thousands of times across a network of computers, and then the network is designed to regularly update this spreadsheet.*[25]

The idea of a blockchain, sometimes referred to as distributed ledger technology (DLT), dates to 1991, when Bellcore (Bell Communications Research) researchers Stuart Haber and W. Scott Stornetta wrote "How to Time-Stamp a Digital Document," a paper proposing practical procedures for certifying when a digital document is created or modified.[26] Hashgraphs are another form of DLT. A hashgraph promises the benefits of the blockchain (decentralization, distribution, and security using hashing) without the drawback of a low transaction speed.

Blockchains and Hashgraphs are immutable—no one can edit a record that already exists; instead, a new record needs to be created to show any corrections or changes to an existing record. That record is then verified for authenticity through a consensus mechanism.

For digital identity applications, there is greater use of permissioned ledgers among trusted parties, as this approach provides increased transaction speeds and improved data privacy. Many proposed blockchain-backed digital identity systems are examples of accumulated IDs, whereby blockchain technology can be used to record transactions between an individual (potentially with no other formal digital identity document) and a peer, service provider, or authority. The history of transactions and

[24] Picture perfect a blueprint for digital identity – Deloitte (November 2018).
[25] Technology Landscape for Digital Identification (27 February 2018). World Bank Group.
[26] www.anf.es/pdf/Haber_Stornetta.pdf

identity attestations, sometimes called *verifiable claims* are built up over time to form an accumulated digital identity.

Though DLT has been around for decades, the technology is only now being explored as an identity trust fabric for enabling individuals to control their decentralized identity, including where and when they share identity attribute information. The advantages to using a decentralized and distributed system for identity verification are that there is no dependency on a single authority, and a person's identity attributes cannot be arbitrarily or abruptly removed.

4. Recommendations

Here are time-tested recommendations for solving digital identity problems that no one company nor one single industry can effectively manage alone.

4.1 Use Open Standards

Open standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption.

Open standards include these traits:

- **Collaborative Process –** Voluntary and market-driven development (or approval) following a transparent, consensus-driven process that is reasonably open to all interested parties.
- **Reasonable Balance –** The process is not dominated by any one interest group.
- **Due Process –** Includes consideration of and response to comments by interested parties.
- **Fair Intellectual Property Rights –** Licensed to all applicants on a worldwide, nondiscriminatory basis, either (1) for free and under reasonable terms and conditions or (2) under reasonable terms and conditions that may include monetary compensation.
- **Quality and Level of Detail –** Sufficient to permit the development of a variety of competing implementations of interoperable products or services. Standardized interfaces are not hidden.
- **Ongoing Support –** Maintained and supported over a prolonged period.

4.2 Collaborate, Don't Isolate

Collaboration and cooperation foster innovation. Coopetition (or "co-opertition") is a neologism that describes cooperative competition. Basic principles of coopetition structures have been described in game theory, a scientific field that received new attention with the 1944 book Theory of Games and Economic Behavior, as well as through the works of John Forbes Nash on non-cooperative games.

Coopetition occurs both at inter-organizational and intra-organizational levels. At the inter-organizational level, coopetition occurs when companies interact with partial congruence of interests. They cooperate with each other to reach a higher level of value creation than the value created without interaction and the struggle to achieve a competitive advantage. Often, coopetition takes place when companies that are in the same market work together in the exploration of knowledge and research of new products, while they compete for market share of their products and in the exploitation of the knowledge discovered. In this case, the interactions occur simultaneously and in different levels in the value chain.[27]

The point of open systems is that they are *open*. Designing the ZenKey mechanism based on open standards and isolating it from the existing ecosystem will only slow and complicate—or potentially halt—adoption. If an ecosystem participant wants to do something special that takes advantage of on-network functionality, then that is fine, but allow for the same kind of functionality that does not require an on-network device. We have to allow other channels; we have to be able to pass digital identity without having closed systems.

> *Overt consumer awareness may help Identity Providers manage the consent workflow and protect their interest, but it places an immense burden on the consumer to remain alert to changing consent contracts. With ZenKey, the carriers may say they are not limiting anything—that they are just not going to work with any intermediaries, and that they will only work directly with the endpoints. But functionally the problem is what becomes of the scenario where RPs must interact with multiple Identity Providers because their IDP of choice cannot interact directly if disallowed by ZenKey.*[28]

4.3 Build Consumer Consent Supporting Multiple Types of Engagement

In many digital identity ecosystem transactions, not all parties have a direct relationship with the user. Without direct user access, for example, the Attribute Provider must rely on the RP to collect a consumer's consent for accessing or verifying their data. When the Attribute Provider is a carrier and the carrier's existing terms and conditions agreement with the subscriber does not already allow this particular use of the subscriber's data, how does the carrier get permission from the user to perform this work?

The most common option at this point is to pass the consent through the RP, which has contact with the subscriber. That requires the RP to collect not just the consent their legal department requires, but also the consent required by the carrier. We have to ask: what if the parameters of the consent (for example, the time period for which the consent is valid) do not match between what the RP collects and what the carrier requires? This scenario is not unlikely and highlights the difficulty and complexity for all parties (including the user) of authorizing every party in a transactional chain.

Over the last five years, immense strides have been taken toward broader use of standards, with the goal of improving the privacy and security of consumer-facing systems. All these new building blocks are still resting on the unstable foundation of the notice and consent constructs underpinning consumer consent management. Despite advances such as MODRNA and FAPI, we are still left with a gaping hole in the foundation on which identity professionals are trying to build a secure wall to protect consumers.

Critical work is needed to develop the standards and designs of a more robust consent management model. Although much is being done to fortify the walls, very little work seems to be in progress to build out this foundational piece of identity management infrastructure. Without redeveloping standards and

[27] "Coopetition Strategy: Towards a New Kind of Interfirm Dynamics for Value Creation" (8 May 2002) EURAM 2nd Annual Conference, Stockholm School of Entrepreneurship, Sweden. Dagnino, Giovanni Battista; Padula, Giovanna.
[28] OIX Interview – Scott G R Rice, PacificEast Research (9 September 2019).

design norms for this critical piece of architecture, the integrity of any identity management design is compromised.

We encourage firms to consider a bottom-up approach to digital identity. First, test and refine the system with a critical mass of parties. Then gradually scale it to include more users, RPs, and Identity Providers. We reiterate our core principles for equanimous digital identity utility:

- Implement open standards instead of proprietary systems.
- Promote open data principles alongside privacy and security.
- Support a range of consumer engagement.
- Provide choice to drive innovation.

By cooperating more broadly with other standards organizations and with de facto standards implemented over time, improved standards and processes can be developed.