Global ID (GID) Framework

Background

Every person has a right, and a responsibility, to a secure, trusted, and private identity. The prevalence of electronic connections implies that we each must identify ourselves to prove our authorization for particular conduct -- without necessarily having to give up any more private details than necessary. For two parties to conduct their affairs in a trusted manner requires balancing reciprocal security and privacy concerns. Age-old concerns about "big brother" have chilled expectations about a corporation or government balancing these competing values. However, the advent of new technologies such as distributed ledgers suggests new possibilities for a universal and *portable* identity solution that does not require a centralized authority. The GID mission is to harness both new technical and governance possibilities to create a "little brother" identity helper rather than a "big brother" identity overlord.

Many of the world's poorer individuals are unable to participate in the connected world, given they lack a digital identity to garner access to particular offerings in society. Nevertheless, even those who have granted access, the status quo is friction laden with redundant signups, as well as susceptible to abuse by bad actors. To date, no one has ever conceived of a central power to do all of this without veering into an Orwellian big brother reality. The alternative of distributed ledger technology and federated governance suggests there is a democratizing bottom-up identity architecture that could include and benefit every member of society.

The GID Framework describes the ability for individuals to control their assets rightly and responsibly as well as permission- based conduct and therefore in turn be trusted by others who do the same. This is only possible by reciprocally balancing the rights and responsibilities of a universal and portable identity framework.

Overview

Global ID (GID) enables each person or entity to own names that are a **secure, private, and trusted means** of controlling one's assets and permission based conduct. Specific names (or tokenized versions of those names) are unique across all use cases and legal jurisdictions in the world. The "**portability**" **of authorization** enabled by names, means that third parties **are no longer required to collect or store personally identifiable information (PII)** to interact safely with GID users.

The ideal GID framework is **governed by all its stakeholders under a federated structure**, rather than controlled by any single corporate or government authority. Access to **underlying data** about **individuals and entities is controlled** by those parties and is only shared and attested by the permission of the party that volunteered the data. While the underlying data is private and secure, **attestations about the veracity of the data are a *public good***, which are openly and equally available to all for the creation of "trust scores" regarding GIDs. Unlike objective attestations about a GID holder, trust scores are subjective interpretations of the value of attestations by a third party who has to decide whether to interact with a particular GID holder.

Privacy rights of GID individuals and entities **are reciprocally balanced with societal compliance and risk controls within the legal and regulatory framework of the user's relevant jurisdictions**. The benefit for Global ID users is that once they join, thereafter they **only have to sign-in to participating services rather than sign-up** and re-enter personally identifiable information (PII). Furthermore, their PII is collected and safely stored once, instead of propagated and exposed across the internet and upon their interactions with service providers. For stakeholders, they also enjoy the benefit of removing friction of new/existing users to access their services, all with higher confidence that those users are compliant and risk appropriate for their offering. Additionally, regulators and law enforcement are provisioned with much more comprehensive and consistent tools. Consequently, they can uphold the law and oversee the risk at hand by **replacing the antiquated and ineffectual limits of silo PII data collection** that is the norm across different countries today.

Attestations, Authentication and Authorization

Each GID identity includes **attestations from third parties who vouch for the authenticity of identity attributes at a particular point in time** (further detail on Attestations on page 7). Presentation of some (secret) attributes associated with an identity constitutes authorized access by the presenting party to act on behalf of the identity in question. Such action may involve the transfer of virtual and material property and/or permissions to engage in particular conduct. Conversely, others may transfer virtual or material property to, and conduct actions directed at particular identities, based on the belief that these destinations accurately represent the person or entity behind the identity in question. Common use case examples are sending funds or viewing documents with a security clearance. Authorized access may be undertaken by the identified party directly or may be pre-delegated via the issuance of tokens ahead of time and for a persistent period, unless the original delegating authority revokes such permissions.

Identity Vaults By Legal Jurisdiction

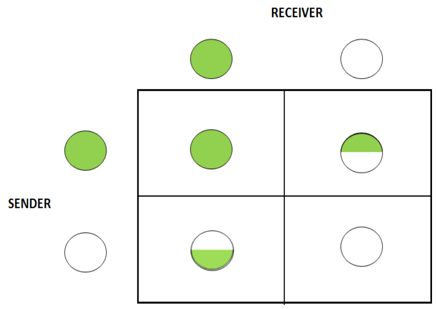
GID is a ubiquitous alternative to silo based identity solutions that previously required each participating party to relinquish PII to each particular corporate or governmental entity with whom they were associated. Alternately, with Global ID, PII is entered by each participating individual or entity and placed first in an encrypted local data store – typically on a local browser or mobile phone under the control of the user. (Further detail on Personal datastores on page 8)**Access to GID data by third parties is regulated by i) the wishes of the party providing those details, including selective access by attestation agents; and ii) by the law of the local jurisdiction in which the data resides due to the activity and location/residency status of the person or entity concerned.**

Only data specifically tagged, as "searchable" via internet-based tools is available via IP based search methods. All other bulk PII **Meta data is unsearchable by design – except through locally running tools that can only be accessed within secure identity vault facilities residing within respective legal jurisdictions**.

Green Ecosystem of Identity

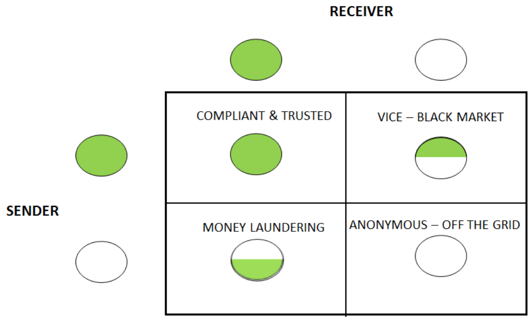
The set of individuals and entities that are sufficiently attested to conduct **secure, trusted and private actions is termed the "green ecosystem"**. There are four states that can exist between two parties that reflect the topology of green versus less than green activity between individuals and entities. In the case of sending and receiving money, the parties can be either rated green (sufficiently attested to) or not (lacking sufficient attestation), resulting in a two by two matrix of possible conduct:

Fig. 1



In Fig. 1, the assumption is that there is a common definition of what attestations are required to be considered green or not green. **Common standards are set as a legal/regulatory standard within a jurisdiction, but also negotiated to a more acceptable international standard when jurisdictions agree to harmonize definitions (as might be the case through an entity like FATF-GAFI (Financial Action Task Force or Groupe d'action financiere))**. Regardless of whether standards for being green are intra- or inter-jurisdictional, the consideration is that the attestations regarding an individual or entity are "pre-staged" prior to authorizing particular conduct by the concerned parties. Pre-staging authorizations is critical to ensure straight through processing for fully compliant and acceptable risk rated activity, but also for intervening with additional enhanced due diligence safeguards or when outright blocking is required.

Fig. 2

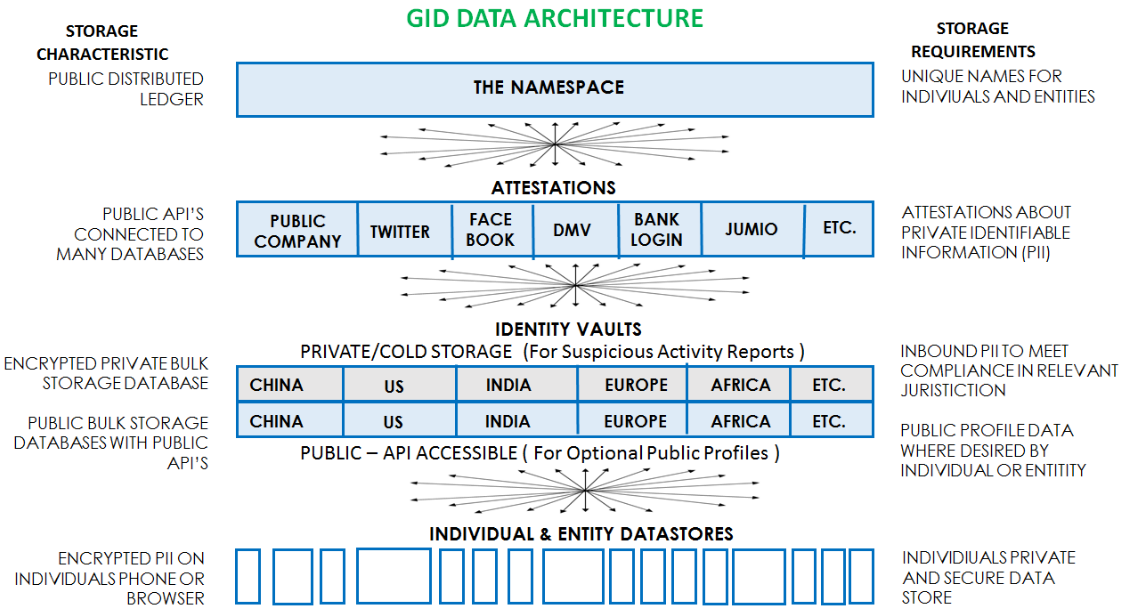


In contrast to **green to green activity that can be characterized as compliant and trusted**, the other combinations of activity that happen can also be labeled to reflect their potential meaning in society. **Green to non-green payments and conduct can be associated with vice or black markets** whereby otherwise compliant individuals and entities seek out non-compliant parties for conduct that is not otherwise authorized in the mainstream of society or the law. Conversely, **non-green to green payments are associated with money laundering of proceeds from vice or black markets** moving back into the green ecosystem. Finally, non-green to non-green payments and conduct are anonymous or pseudo anonymous and operate "off-the-grid" from the green ecosystem of identity attestation.

The GID Architecture

The GID architecture is composed of **i) a namespace on a distributed public ledger; ii) attestations about those names via APIs; iii) compliant identity vaults for each legal jurisdiction served; and iv) user controlled personal datastores of personally identifiable information (PII).**

Fig. 3


GID DATA ARCHITECTURE
STORAGE CHARACTERISTIC
PUBLIC DISTRIBUTED LEDGER
THE NAMESPACE
STORAGE REQUIREMENTS
UNIQUE NAMES FOR INDIVIUALS AND ENTITIES
ATTESTATIONS
PUBLIC API'S CONNECTED TO MANY DATABASES
PUBLIC COMPANY
TWITTER
FACE BOOK
DMV
BANK LOGIN
JUMIO
ETC.
ATTESTATIONS ABOUT PRIVATE IDENTIFIABLE INFORMATION (PII)
IDENTITY VAULTS
PRIVATE/COLD STORAGE (For Suspicious Activity Reports)
ENCRYPTED PRIVATE BULK STORAGE DATABASE
CHINA
US
INDIA
EUROPE
AFRICA
ETC.
INBOUND PII TO MEET COMPLIANCE IN RELEVANT JURISTICTION
PUBLIC BULK STORAGE DATABASES WITH PUBLIC API'S
CHINA
US
INDIA
EUROPE
AFRICA
ETC.
PUBLIC PROFILE DATA WHERE DESIRED BY INDIVIDUAL OR ENTITITY
PUBLIC – API ACCESSIBLE (For Optional Public Profiles)
INDIVIDUAL & ENTITY DATASTORES
ENCRYPTED PII ON INDIVIDUALS PHONE OR BROWSER
INDIVIDIUALS PRIVATE AND SECURE DATA STORE

The Namespace

The namespace is where **individuals and entities unique names are displayed and "owned" using cryptographic signatures**. The list is a **public good** in which everyone has access – the **prime benefit** being assurance regarding **who owns a particular name at a particular point in time** (and secondarily for how long they have owned that name and any attestations that create a trusted reputation around that name)

Significantly, the existence of a name is not an indication that someone is a good rather than a bad actor. The **sole purpose of the namespace is to unambiguously designate who has ownership** of a name, independent of any value judgment that can be reached about the owner.

Furthermore, the existence of a name is **not an assurance, in itself, of identity in a manner that "outs" the owner of that identity in a personally identifiable form to the public**. While a particular name may be purposely tied to other information that is shared to advertise a brand or personal reputation, the exact opposite use of the namespace as a privacy enhancing mechanism is also supported by the namespace. A name can purposely represent a level of indirection between a true identity and a privacy enhancing alias under which someone operates in their daily life (but which could still be tracked back on a need-to-know basis if a crime has been committed).

The aspirational design is that **everyone and every entity (and potentially everything in the internet of things) should want to have one or more names – some more public and some more private** – so that they can more easily prove (perhaps while maintaining privacy) themselves and their associated permissions when attempting to take action with others.

Distributed ledgers make equal, open, neutral, and permission-less access to this information (**in real time**) available to everyone and everything in the world. A decade ago, this method was impossible and therefore never contemplated as the foundation for a global identity framework. However, today **founding an identity framework on distributed technology (and governance)** is not only possible but an imperative in **a multilateral world** where there is no single authority on identity.

Attestations

Attestations are **signed statements (by a user and a third party) about the objective state of some aspect of that user's PII**. Notably, **attestations are *not* the PII itself, but rather some verification or validation about that PII**. Thus an attestation can state that particular PII exists and/or is judged to be accurate **without i) giving up what that PII is, or ii) making a subjective judgment about whether the objective attestation means that the party concerned is a good or bad actor**. Attestations should not be confused with ratings, which are the subsequent (and subjective) ascription of good/bad absolute and relative scorings – which is beyond the scope of the GID Framework, but represents fruitful grounds for 3rd parties seeking to offer those value added services.

Attestations are about names written to the namespace, but attestations need not live in the namespace as long as they are cryptographically signed *about* a namespace entry and live in an API accessible database. As long as those attestations can be reached by 3rd parties in a timely fashion, then the need to support ratings and other on-demand issuance of permissions is met.

Personal Datastores and Identity Vaults

A **personal datastore describes the practice of an individual securely and privately storing personally identifiable information (PII) about themselves in an encrypted form on their local browser or a mobile phone**. As such, the information is retrievable and sharable by them only when they authorize such activity – and is otherwise private. Having entered and saved the data, the user in theory would not need to re-enter it other than to update or cope with a lost or new local device that holds the datastore. The user unplugging from the internet (cold storage) or erasing the datastore altogether could disconnect personal datastores from access to the outside world.

Personal datastores are privacy enhancing but fall short of meeting compliance requirements in various legal jurisdictions for conducting particular types of activity in society (sending and receiving money, boarding an airplane, etc.) that involve trust with third parties, or compliance with laws regarding illegal or terrorist activity. Thus, individuals and entities that wish to partake in societal activities inevitably have to give some PII to a third party. Historically, such PII would have to be given to each 3rd party service provider to store in a database controlled by that 3rd party. Such databases of PII become the target for hacking attacks given that such information can aid in identity theft and other malicious behavior. **Rather than multiplying the copies of PII every time a user interacts with a 3rd party service provider, a single or few carbon copies of PII could be kept in a purpose built "identity vault" accessible only on a need-to-know basis with due process of law and/or consent by the user in question**.

Identity vaults operate as a log of every piece of PII that is volunteered by the user about themselves (date stamped for any time changes**). No information in an identity vault is obtained from any place other than the user themselves**. In contrast to a credit bureau that is built from 3rd party sources about a user, an identity vault provides the opposite function – a store of data volunteered only by the user themselves. Furthermore, every user has a right to see (and edit) every piece of information about themselves – although an audit trail of all changes is always recorded to maintain present and past state of the identity data. Whereas credit bureaus are littered with erroneous and outdated information about a user, an identity vault is completely managed by a user themselves – implying personal responsibility (and empowerment) for the provision of accurate and up to date data. The role of 3rd party attestations is segmented from the vault itself so that there is a divide between provision of privately identifiable information and the verification of that data by 3rd parties.

All data in an identity vault is nothing more than what the user could/would have stored about themselves in their own personal datastore. The advantage and need for an identity vault (in addition to a personal datastore) can be summarized as:

i) **The identity vault is available 24/7** from an easily accessible (namespace directed) API so that attestation agents can easily (and with user permission) access PII necessary to timely undertake a particular attestation. A personal datastore might (or might not) be available at a particular point in time to facilitate such a request and therefore is operationally inadequate for some situations

ii) The **identity vault ensures that particular data necessary to meet CIP/BSA/AML requirements is accessible by firms** for suspicious activity reporting requirements. Unless such data was guaranteed to be available, PII data would have to be collected and stored directly by firms providing services to users -- which would degrade privacy protections and increase security vulnerabilities

iii) **Users who want to promote a portion of their PII details in a public profile or brand can dynamically attach their profile, address book entry, web identities, etc. to the underlying data contained in the vault**. Additional third party registries can (with permission) also build offerings based on the publicly designated data elements in the identity vaults. Thus Skype, Twitter instant message, mobile address books, and other profile based services can leverage public facing identity vault data to build out more trusted profiles of their users (when those users grant permission to do so)

OAuth for Portable Identity

The greatest user benefit of the GID framework is reduced friction without increasing risk when signing up or using existing services from third parties. The key mechanism behind enhanced access is a standardized process for identifying oneself when seeking authority to enjoy certain permissions and undertake certain actions.

Rather than having each stakeholder run their own authorization system for accessing products and services, the GID Framework supports OAuth – essentially a Facebook Connect like ability to proxy authorization for entry into a system based on secure details that are hosted elsewhere by a trusted third party. However, **whereas Facebook OAuth is more about verification from an entity holding your social network credentials, the GID OAuth Framework involves higher stakes related to the controls over access to all your funds and potentially your ability to prove permission to life-or-death capabilities**. It is almost certain that the need for digital identity for such serious/higher stakes matters will only increase. The GID OAuth Framework also signals to the custodians of your funds and entities that give your access permissions that they can trust that you are really you (or an authorized designate) and should be given full access to the capabilities you expect to have once that proof has been demonstrated.

At a minimum, a user's **GID OAuth credentials** imply the entry of usernames and passwords (typically **overlaid on public / private key cryptography**). For convenience and situations demanding **more certainty and security, additional tokens of one's identity (such as email or phone confirmations) are likely to be enforced. In addition, for even higher risk situations, multi-signature requirements and/or biometrics may be additional**

requirements to establish authorized access to funds or capabilities associated with a particular namespace.

Historically, OAuth defenses were associated with traditional centralized actors (Facebook, Google, Twitter) that could vouch for the user's logging in at third party sites to prove their identity. These lightweight implementations have generally stopped short of assurances required when dealing in mission critical situations that could include regulatory requirements or national security. For **GID OAuth, higher levels of security, coupled with privacy safeguards, are needed**. Also relevant is GID OAuth can take advantage of new technologies for **generalizing the notion of a global namespace and of trustless registries of names and other attestations** that simply did not exist at the inception of Facebook and Twitter.

GID Offerings Besides OAuth

GID **operates a dual issuance namespace** on **publicly accessible distributed ledgers**. Once names are issued on the **"raw" ledger**, the **recipient receives a private key that ensures that they, and only they, can allow attestations** about their name or transfer it to another party. In parallel to issuance of names on raw ledger, a parallel "**curated" ledger** entry is made for **which GID, rather than the name user, controls the secret key**. Under normal conditions, the curated version of the namespace will match the raw, but in the event of a proven claim that a raw name's access has been lost or stolen; **the curated version can denote the discrepancy.** GID can make a decision to re-assign a disputed name on its version of the ledger, in response to due process of law. **Third parties can choose to rely on only the raw version of the namespace or reference GID** (or competing curated interpretations) **of what ownership should be if/when law overrides raw permissions state** of the ledger.

The GID Framework purposely anticipates the tension over a technically pure and permissions based view of the world where he/she who has a secret key trumps any other considerations about law (i.e. a view in which possession is 100% determinant). The GID counterbalance is that rules and law by various jurisdictions can determine who truly has authorized access to a name and attendant attestations, especially when the associated secret keys have been compromised or misappropriated by coercive and/or illegal means.

GID arbitrates disputes over namespace allocations when trademark or unauthorized conveyance is an issue. Because ownership of a name sits on a public ledger that states the duration of ownership of any particular name, it is easy for any and every one to determine which names (and their attendant attestations) have a long and durable track record versus those that have been hastily created or transferred. Names with longer and stable attestation histories are much more likely to be trusted than newly created or recently transferred names, which may enjoy little or no trust at all. Importantly, because the namespace registry is updated in near real time, there should never be ambiguity as to whom the actual holder is of a name that may be designated with particular permissions, including the receipt of funds being sent or spent.

GID names are issued free of charge and are renewable each year. Individual users are expected to **limit their collection and use of names to five per person (ten per entity)** though a waiver of the limit can be applied for in special circumstances. Each GID name is expected to be attached to a mobile phone number and an email address at a minimum so that the maximum issuance thresholds can be observed and administrated. The **issuance of one time (disposable) names is available to already established users** with a track record of good behavior. These onetime names can automatically inherit a set of attestations that will signal that the holder is well attested to but seeks to use a one time (privacy guaranteeing) token name for a particular transaction rather than a persistent name. Onetime names can be mapped back to the original persistent name holder only when suspicious activity has been detected with a particular person or transaction and due process dictates replacing the disposable name with the more persistent named party that asked for a one time token name.

GID certifies which attestation providers are acceptable to participate in the GID framework. GID has no power to prevent non-certified parties from hosting their own attestations about namespace entries (which are publicly accessible to any or all). However, only certified attestation agents will be treated as GID constituents with full shareholding and governance rights. GID will actively resell attestation services of all constituent members and will ensure that access to an attestation agent's information is available through default API offerings for the GID ecosystem.

Individuals or entities who have been attested to can choose to notate that particular attestations as no longer (in their belief) accurate or relevant. GID will denote all user expired/revoked attestations as indicated, and compliant rating services will respect the request to not include user expunged attestations in any rating score calculation.

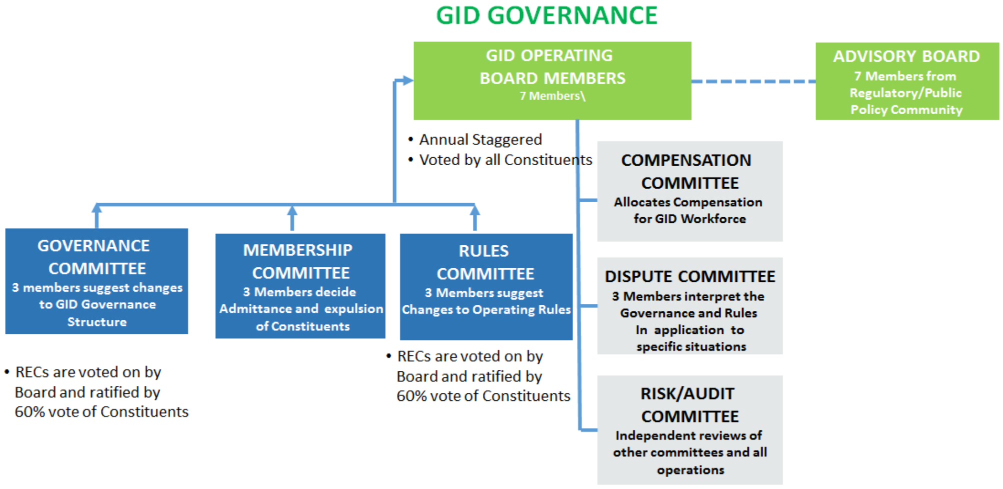
GID certifies identity vault providers that are deemed acceptable holders of PII in the various legal jurisdictions from which end users originate (essentially every country in the world). PII in certified identity vaults is accessible via GID specified APIs for access by certified attestation providers when combined with end user wishes that such data be accessed to obtain a particular attestation.

GID sets pricing for attestations requested by stakeholders seeking such attestations. **GID also sets pricing for access to identity vaults by stakeholders** needing to conduct suspicious activity reports. **GID provides identity vault services for the holding of PII to end users for free** and recoups the costs through marking up attestations about the PII held in identity vaults. All users are thus incentivized to utilize free identity vaults and to keep comprehensive and up-to-date PII. GID also offers optional interchange priced insurance and assurance services for stakeholders using GID OAuth services when conducting permission based activities where GID's risk and compliance controls are utilized.

GID Governance

After an initial setup period spearheaded by GID founders, **GID operates as a stakeholder governed entity with advisory input and effective oversight from members of the regulatory and public policy realm**s. GID is **led by an "Operating Board" elected by its constituents**. The Operating Board makes majority decisions on key rulings, which in turn are ratified by a 60% majority vote of stakeholders. A dotted line relationship exists with the independent Advisory Board composed of present and past members of the regulatory and consumer advocate community.

Fig. 4


GID GOVERNANCE
GID OPERATING BOARD MEMBERS
7 Members\
ADVISORY BOARD
7 Members from Regulatory/Public Policy Community
• Annual Staggered
• Voted by all Constituents
COMPENSATION COMMITTEE
Allocates Compensation for GID Workforce
GOVERNANCE COMMITTEE
3 members suggest changes to GID Governance Structure
MEMBERSHIP COMMITTEE
3 Members decide Admittance and expulsion of Constituents
RULES COMMITTEE
3 Members suggest Changes to Operating Rules
DISPUTE COMMITTEE
3 Members interpret the Governance and Rules In application to specific situations
• RECs are voted on by Board and ratified by 60% vote of Constituents
• RECs are voted on by Board and ratified by 60% vote of Constituents
RISK/AUDIT COMMITTEE
Independent reviews of other committees and all operations

A **Governance Committee is responsible for the Governance Charter of GID. T**his includes being responsive to changing needs of the entire stakeholder community and the mission of achieving a "public purpose." The Rules Committee is charged with resolving the daily GID Operating Rules that govern the operational activities and interactions of the organization. Both committees bring their recommendations to the Operating Board for a majority vote, and then must achieve 60% acceptance by the stakeholder community for final passage.

The **Membership Committee determines which attestation agents, identity vault providers, stakeholders, investors, and core members** are acceptable for membership in the GID framework. The Compensation Committee determines the allocation of GID earnings disbursed among members of the Core team, the investors, and the stakeholders.

The **Dispute Committee handles the aforementioned disputes over the ownership and transfer of names in the namespace as well as disputed claims for access to user PII from 3rd party individuals, entities and governments**. Finally, the

Audit and Risk Committee provides a review of all other committees and operating functions within GID, but also of constituent activities, particularly with regard to security and privacy controls.

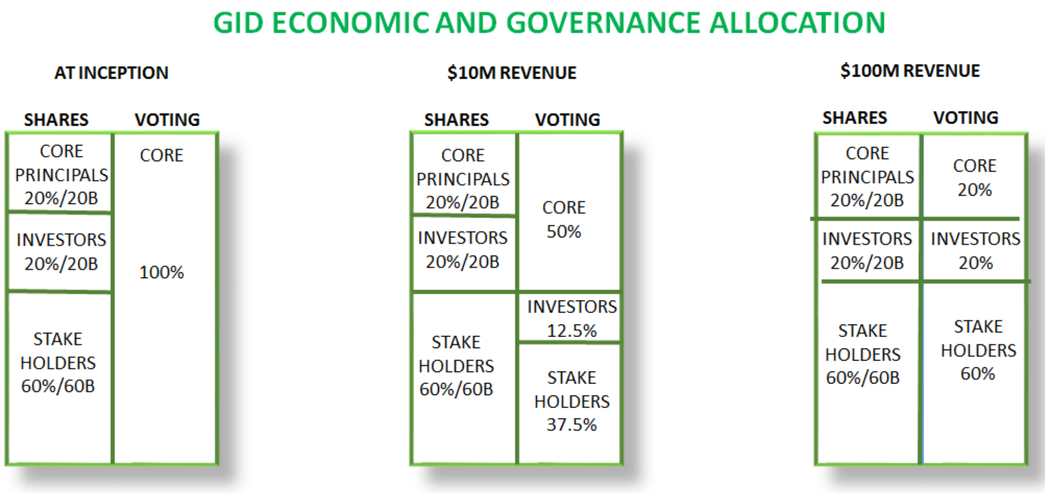
Out of scope for this paper is a description of the actual GID operating company, which runs GID on a day-to-day basis.

GID Ownership and Voting Rights

As a stakeholder driven entity, **the long-term ownership and voting rights of GID is heavily weighted to represent the stakeholder constituents**. Carve outs are also provided for investors that provide the working capital for building and growing GID (until it becomes self-sustaining), as well as the core team of individuals that lead and manage the entity.

To jump start the GID framework, decision making (i.e. voting) is initially concentrated 100% in the leadership team until a $10M run rate is achieved, at which time 50% of the voting rights are available to the participating investors and stakeholders. When a $100M run rate is achieved, the assumption is that GID can realize its full stakeholder mandate and interlock ownership and voting rights 1:1 at a target ratio of 60% for stakeholders, 20% for investors, and 20% for the Core GID principals. It is anticipated that payouts of earnings from GID operations will be made to active (rather than passive) Core members – a determination that will be made by the Membership committee (re: active versus passive status) and the Compensation Committee (proportion of returns allocated between individuals based on level of effort/contribution to the cause). The only passive payouts of GID returns will be to investors who have contributed either money or services-in-kind to the building of GID in expectation of a return on investment.

Fig. 5



A grant of 100 Billion share/currency units as a surrogate for ownership is recorded as registry of both economic and voting rights. The share units are held in custody (rather than distributed) on a For Benefit Of (FBO) basis for Stakeholders and Core members. Investor's holdings are freely tradable in the open market and as such will find a market price for their value, and so, in turn, for the GID Framework.

Summary

It is the positioning of the GID Framework as a public good that is the key differentiating feature from other, prior, and centralized efforts, to create an identity solution for the world. An identity solution that happens to be portable and controlled by end users themselves while still not only meeting the needs of FIs, regulators, consumer advocates, and other stakeholders, but also including them as part of the Federated Advisory structure and Board.