The Namespace for Identity

Overview

Every individual and entity has a unique ***name***. This name represents the owner's identity. The name we create for ourselves belongs to us and transcends national and corporate boundaries. Taken together, the pool of all registered names constitutes a global ***namespace***[1] for identity.

In this paper, we introduce globaliD's ***Identity Name System*** (INS), see how it supports the three main pillars of identity — privacy, security and trust — explore how names work within the INS protocol, and see how INS can lead us to a world no longer rife with spam, fake news, fraud, money laundering and the like.

The Identity Name System

The Internet's ***Domain Name System*** (DNS) is used to map human-comprehensible names such as `google.com` to the underlying address for the associated web site. In the same way, the ***Identity Name System*** (INS) maps human-comprehensible names such as `bob_smith` to the underlying identity associated with that name. INS is designed to mirror the scope and reach of the Domain Name System, giving every person and every entity an identity linked to a unique name. In this way, INS allows identity to be ubiquitous, humanizing and easy to use.

Ultimately, the INS registry of all names and their associated identities is a ***public good*** — that is, it is openly, equally and freely accessible to all.

---

[1] Examples of namespaces are the collection of all Twitter or Skype names, which are unique identifiers within their own ecosystem but not necessarily across other platforms.

The Three Pillars of Identity

An identity system has to encompass three main virtues, which we will call the ***pillars of identity***:

- ***Privacy:*** Since the end user has to provide information about themselves, how can the identity system ensure that this information is kept private so the user is comfortable providing this information?

- ***Security:*** Once information has been shared, there is no telling where that information will end up or how it will be used. Information held on remote servers is also a target for hackers, and there have been numerous cases where private data has ended up in the hands of spammers and scammers.

- ***Trust:*** The whole point of an identity system is to allow a web site or application to control who can do what. The site or app needs to trust that only suitably-authenticated and authorised people can perform a given action, and users need to trust the site or app not to abuse their data.

All too often, these three pillars are seen as competing trade-offs rather than as complementary virtues. For example, in order to trust that only licensed drivers can hire a vehicle, a car hire firm may require the user to submit a copy of their driver's license. That license typically contains the driver's name, address, date of birth, photograph, and a copy of their signature. Once this information has been captured, it may well end up being stolen or used inappropriately. In this way, trust and privacy are seen as competing opposites, with security the poor piggy in the middle.

Instead of viewing privacy, security and trust as incompatible values to be traded off, INS treats them as mutually reciprocal: through preserving privacy, trust can actually be enhanced and security can be maintained. Let's take a closer look at how this works in the INS world.

Privacy

The key to privacy within INS is through the concept of ***attestations***. Each attestation is a securely-made claim about the validity of some piece of information about the identity. For example, upon submission of a verified date of birth, a third party may assert that the holder of the name is over 18. This claimed fact, "is over 18", is an attestation. Attestations are always public — anyone can view the list of attestations associated with a name — while the underlying personally-identifiable information (in this case, the date of birth) is private and is only ever seen by the third party making the attestation.

An attestation is more than just proof that the user was able to provide a piece of information. Anybody can take a photo of someone's valid driver's license or type in a random phone number. To obtain an attestation, the user must prove that they control or have legitimate access to that piece of information. In the case of a phone number, this involves an automated process of sending an SMS message to that phone number and requiring the user to enter a random number included in that message; this has the effect of proving that the user not only knows the number, but can receive messages sent to that number. For a driver's license or other type of photo ID, the user must take a selfie of their face using their mobile phone, and that image must match the person shown on the ID. In this way, the attesting party can be confident that the user can not only provide some information, but that the information is valid and belongs to that user.

Using attestations, privacy is automatically preserved by only revealing the attestations about an identity, rather than the underlying personally identifiable information. In this way, information such as an email address or mobile phone number can be confirmed for an INS

name without ever revealing these privacy-compromising details to a stalking- and spam-prone world.

Security

In a non-INS world, users often have to reveal private details about themselves before they are allowed to perform an action. Once revealed, the user has no control over how their data is used. With INS, only the public attestations are revealed, and the user's data is kept secure.

Data breaches are another major security concern. If an app or web site stores user data in the cloud in a form where it can be accessed by that app or web site, then an intruder can and will break in and steal it. A user's data is only as secure as the server on which it is stored — and server intrusions are common. Almost every week, another major data breach is discovered, and thousands or even millions of users discover that their names, email addresses, passwords, credit card numbers and other details have been stolen.

Security is only as strong as its weakest link. Even with encrypted data, if the key needed to decrypt that data can be obtained by an intruder then the encryption is useless. With INS, the user's personal data is encrypted and backed up to the cloud, but the key needed to decrypt that data is only held by the owner of the name[2]. The only exception is the additional cold storage of particular data elements needed to meet AML/BSA/KYC requirements in the legal jurisdiction where the user resides.

[2] An additional copy of the user's key is split into multiple parts and shared between several of the user's designated contacts. If the user loses their key, they can ask their contacts to provide their portion of the key, allowing the key to be reconstructed. This, however, requires the agreement of multiple contacts, all of whom must be convinced that the request is legitimate.

Trust

Permissions are based on trust: before granting permission for a given user to perform a given action, an app or website needs to trust that user is (a) who they claim to be, and (b) authorized to perform that action. Trust, therefore, has two components: authentication and authorization.

Authentication is the process of ensuring that the given user is indeed the legitimate owner of a name. Let's assume that the name `jeff_bezos` has a rich and powerful collection of attestations associated with it. If I could claim to be Jeff Bezos simply by typing in that name, or more likely by writing a computer program that masquerades as that name, then any system which relies on attestations associated with a name would let me do things I shouldn't be able to do. Authentication, therefore, is a crucial first step in building trust.

With INS, authentication is achieved through a process known as *tokenization*. Tokenization is based on industry-standard cryptography techniques: the owner of a name has a private key which is used to prove ownership. This private key is stored securely on a device such as a mobile phone, on a smart card chip, or embedded in a wearable device. The phone, card or device then becomes a "token" for the name — possession of the phone, card or wearable device, along with the ability to pass biometric or PIN code tests needed to unlock the item, proves that the possessor is indeed the owner of the name. Instead of relying on something you *know*, for example an easily-hackable username and password, INS authentication relies on something you *have* — an identity token which you have proven ownership of through the use of a biometric or PIN code test. This helps to ensure that you are indeed who you claim to be.

Authorization is the process by which an app or website checks that a given user is allowed to perform a given action. With INS, this is done by checking the attestations associated with the user's name. Attestations prove that a given piece of information about a particular name holder was valid at a particular point in time. Collectively, the attestations associated with a

name give that name a *reputation*. Using this reputation, an app or website can decide whether or not to allow the name's owner to perform a given action. Different actions require different levels of trust, along a spectrum of riskiness. For more risky actions, it is possible to require multi-token confirmation[3] and/or co-signers[4] as additional safeguards. This helps to protect against unauthorized or coerced use of the user's identity token.

A name with no attestations at all has no reputation, and so that name's owner will be able to do almost nothing with that name. By garnering attestations, however, the name's owner can build up their reputation to the point where third parties can rely on those attestations to trust the name holder to perform various actions. In this way, a highly-reputable name is valuable in that it allows the name's owner to perform more actions.

Note that, unlike a credit score where third parties can attach negative information to an identity, the INS protocol and attestation database is *self-sovereign* in that a named person can always choose which attestations about themselves are added to the public registry. An individual may choose to record as few or as many attestations as they wish. However, a sparsely-attested-to identity is less likely to be seen as trustworthy and so will receive fewer permissions when the context of local laws require a more robust set of attestations. Having a long-lived but imperfect reputation may be more trusted than having a clean but newly-created or sparsely-attested-to name. Simply creating a new named identity to replace a long-established but tarnished one is ultimately self-defeating as it merely highlights the sparse track record associated with “burner” names.

[3] An example of multi-token confirmation includes confirming that a payment card is physically present at the same location as the merchant terminal in addition to the mobile phone of the payor (on which an encrypted globaliD token is embedded). A further confirmation might include a biometric check of the user to match against a prior attestation on the user's phone.

[4] Co-signers may include persons that a user previously designated from their contact list as trusted co-signers. For particularly risky actions, multiple co-signers may be required.

How INS Names Work

Within INS, names are unique “handles” rather than having to be actual names of real people or entities. While no two people or entities can have the same name, it is possible for an individual user to have multiple names, each for a different purpose. For example, one name may represent the user's business, while another represents his or her personal identity.

Each of a user's names is distinct. That is, the attestations associated with a name are unique to that particular name: for each name, the user's personally-identifiable information can be used to generate attestations for that name, but if the user has multiple names they will have to generate attestations for each of their names in turn.

One of the key tenets of INS is that there is no way of knowing that two or more names are owned by the same person. Because only the public attestations are revealed and not the underlying personally-identifiable information, it is impossible for an outsider (or even an intruder into the INS system) to discover that two names belong to the same individual. This is vital when it comes to maintaining the user's privacy, and can even have safety implications in societies or domestic situations where a second, "secret" identity can be used as a means earn freedoms that would otherwise be taken away.

Just like website domain names, INS names can be ***transferred*** from one owner to another. Ownership of a name would usually be lifelong, but for role-based names ownership can change with circumstances — for example, the name "POTUS" (President Of The United States) may be transferred to a new owner after an election. A name may also be transferred when a business is sold, or in any other situation where the current owner agrees to give the name to someone else.

When a name is transferred, all the public attestations about that name are also transferred to the new owner. Most crucially the underlying personally-identifiable information is not transferred. In this way, the name has a ***trail of provenance*** that stays forever with that name. Because the attestations are preserved across the change in ownership, an understanding of why authorizations were granted for things such as funds moving between parties, missiles being fired, etc, can be maintained in a world of rules and laws.[5]

While it is a matter of public record that a name was transferred to a new owner, this may or may not affect the name's reputation. For names representing branded entities, the reputation of the name may have an enduring provenance that is stronger and more persistent than the ownership of that name by one particular individual.

As well as transferring names to a new owner, a name's owner may choose to ***release*** a name they no longer want. When a name is released, the name goes back into the pool of names which others may claim as their own. Taken together, the three processes of claiming, transferring and releasing names allows a user to set up the identity or identities which they want to control, and keep these identities relevant over time.

Finally, because names are tokenized onto devices, the loss of a device could potentially mean that the user loses control of their name. As soon as a device has been lost, stolen or compromised, the user can immediately ***revoke*** the name(s) held on that device. That renders the name or names unusable, preventing anyone who has the device from using those names, even if the built-in biometric and other checks on the device are bypassed. Once the user has a new device (or regains control of their existing device), they can then choose to ***restore*** their name(s) onto that device. As well as quelling security concerns, revoke and restore allows users to keep their INS names when upgrading to a newer phone.

---

[5] Europe's GDPR regulation for the right to be forgotten implies that a user may request that their personally-identifiable information can be hidden or removed at their discretion. While INS allows for this, the fact that a particular attestation was generated at a particular point in time is immutably recorded into a blockchain so that third parties can determine that the public history for a name has not been altered, even if the personally-identifiable information associated with those attestations have subsequently been removed. The only exception to this right to be forgotten is the regulatory-mandated preservation of information of "legitimate interest" needed to meet AML/BSA/KYC reporting requirements.

INS as the Path to a Better World

One has only to look back at the pre-DNS world to understand the consequences of continuing our current fragmented identity path. Prior to a global namespace for domain names there was no World Wide Web, and society made do with fractured and siloed communications networks like AOL and the French-based Minitel. Had people been satisfied with these locally-optimised solutions, there would likely not be the ubiquitous and inclusive internet that we enjoy today.

In terms of identity, the equivalent of AOL and Minitel are corporate and governmental silos such as Facebook, WeChat, and the India-based Aadhaar. While these systems work at one level, they actually impede the path to a global and inclusive identity protocol, one that is privacy-preserving, secure, and ultimately trusted.

INS provides a better path. By using unique names and associated attestations, the reputation of actors can be understood and actions allowed or blocked accordingly. This is a real rather than a window-dressing defense against bad actors, who otherwise would play havoc with fake news, fraud, money laundering, terrorist funding and other coercive and abusive behavior. The inappropriate use and leaking of data, as exposed by cases such as Facebook and the Panama Papers, becomes exponentially harder when INS-verified names and attestations are required for particular actions that pose a risk to people's privacy and security. Furthermore, the use of long-lived names with a rich history of attestations helps to build trust that, not only is someone who they claim to be, but that they will continue to behave in a reputation-enhancing way in the future. In this way, privacy, security and trust are grown rather than traded off.

One of the key ideas behind INS is that it is ***ubiquitous***. Rather than only including a particular subset of people and entities who happen to want to use a particular system, or who reside in a particular country, an INS name is available to anyone. This includes the poor, and those from countries or in circumstances where they would ordinarily be excluded from traditional identity

systems. This allows everyone to experience the freedoms and responsibilities associated with having an identity. By selecting a name and anchoring attestations to that name, anyone in the world is able to build a reputation that can allow or prevent that person from performing various actions.

An identity ecosystem is enhanced not by excluding problematic actors, but by deliberately including all — and in particular, bad — actors. Named bad *actors* are meant to be in a system that limits bad *actions* by restricting their permissions. To achieve this, the bad actors' named identity must be confidently known so that their permissions can be limited to match their reputation.

The concept of good and bad actors depends on context. This means that the INS protocol itself does not attempt to classify actors as good or bad. Because attestations are inherently *neutral*, they can be used by different countries and regimes to identify the set of individuals and entities which fall under their jurisdiction, while ignoring those names which don't meet their requirements. It doesn't matter whether a particular regime is privacy-preserving or privacy-shredding, libertarian or totalitarian — either a given name has the attestations required for a particular permissioned activity in that jurisdiction, or it does not. This allows corporate and government rules to be respected, with permissions granted or denied accordingly.

The key difference with INS is that named identities are both persistent and portable, allowing them to be used across all legal and corporate regimes without having to be reconstructed from scratch. The attestations built up over time form a "bundle of sticks" that the user can bring to any table. If those sticks are sufficient to allow a permissioned activity, then permission is granted. If not, then the user can either seek out additional attestations to meet the regime's requirements, or else decide that the permissioned activity isn't worth the effort and abandon the request. Either way, both parties have exercised their free will in deciding whether or not to go ahead with the activity.

In tribal times, everyone in a tribe had a unique name, and everyone had a reputation that was known by all. There were no problems with duplicate names or uncertainty as to someone's reputation because tribes were small and everyone knew everyone else. If two tribes both had members named Joe, it didn't matter because Joe at tribe A would never be confused with Joe at tribe B, especially then the primary interaction between the two tribes was war over territory and spoils.

In today's world, however, people interact and do business all over the globe. Just as DNS operates in a simple but expansive manner across the world, INS operates in a global sphere where interactions across boundaries is the norm rather than the exception. Parochial company and even national thinking cannot become speedbumps, let alone walls, to global interactions. Unlike these siloed systems, the global INS protocol is a transformative solution that sees privacy, security, and trust as mutually reciprocal rather than competing values.

The simple aim of INS is to ensure that it is easier to build and maintain a good name rather than starting anew after debasing a prior name. While making it more desirable to maintain a good reputation in a name rather than rebuilding from scratch may seem like a fairly humble goal, the success of DNS in promoting the trust and adoption of a ubiquitous namespace for websites is instructive and compelling as a dry run for what INS should aim to achieve.

Summary

We have naturally placed our trust in various institutions. Many of these institutions have proven to be complicit in, rather than rooting out, fake identities. This problem has become so widespread that we can no longer trust the systems upon which we rely due to a significant proportion of rigged players. It was bad enough when the siloed nature of identity meant it was easy to commit fraud, launder money, finance terrorism or conduct criminal activity. Now, the stakes have grown to the point of undermining our trust in mainstream media and even

voting systems. As a society, we need the INS protocol as the foundation for rebuilding reputational trust in names and entities, and all the activities on which these are based.

INS builds on what worked for our ancestors: names, registries, and independent and provable attestations about a name. DNS suggests that this can and should be done at a global scale to replace the failing status quo of corporate and national identity silos that may have worked well enough in a less connected past, but fall well short today and in an even more challenging future.