The Tokenization of Identity

What is Tokenization?

In the globaliD world, everyone has a name that uniquely identifies them within the system. But how can someone prove that they are the legitimate owner of a given name? To do this, the user has to ***authenticate*** themselves to prove that they are the legitimate owner of a given identity. There are two ways in which this authentication can be performed:

- By relying on something the user ***knows***.
- By relying on something the user ***has***.

The former is the traditional username/password approach to authentication, relying on information that the user knows and that no one else is supposed to know. In the latter approach, the user possesses something that acts as a ***token*** for their identity. In this paper, we will explore the concept of identity tokens and how they provide a superior means of authentication compared with the traditional knowledge-based approach.

What is an Identity Token?

Every identity has a unique name. Associated with that name is a public key that can be used to securely interact with that identity. Both the name and the public key are (by definition) public, and can be found in the globaliD Namespace.

Also associated with the identity is a corresponding private key. The private key is literally the key to the user's kingdom: the holder of the private key is considered to be the legitimate owner of the identity, and can perform actions and access all information held about that identity.

While the private key could theoretically be printed out or shared, it can be used as an identity token by embedding it into a physical item or device, for example by recording it into the magnetic strip on a card, storing it on a mobile phone, or encrypting it onto a wearable or carryable device. The item or device then acts as a ***token*** for the identity, and possession / ability to use that device is considered to be proof that the bearer of that device is the legitimate owner of the associated name.

Using an Identity Token to Establish Trust

Mere possession of a card or a mobile phone is not enough to establish trust that you own the identity represented by the token embedded in that card or device. To do this, you first need to ***authenticate*** yourself with that item or device. For a card, this might be done through the entry of a PIN code. For a mobile phone or wearable device, this can be done through biometric authentication such as a face or thumbprint ID. If you are able to pass this authentication step, then this establishes a base level of trust that you do indeed own the identity tokenized within that item or device.

For particularly risky actions, multiple forms of authentication may be required. Multiple tokens may need to be presented before authentication is sufficiently robust to grant authorization. For instance, when a tokenized card is presented in a brick and mortar store, the GPS coordinates of a tokenized phone may be uploaded (with the user's consent) to prove that the phone is at the same location as the payment terminal being used. The existence of two identity tokens gives the shop owner more assurance that the payer is the legitimate owner of the proffered identity.

Taking this concept even further, a particularly risky action such as sending a very large sum of money from one entity to another, or firing nuclear missiles, may require multiple signatures from different named and authenticated parties before authorization is granted.

Transferred Authentication

An identity token can be used to ***transfer*** authentication to another device, allowing the permissions granted to the identity to be used on a device other than the device holding the identity token. This is done through a mechanism we call ***globaliDConnect***: the user first establishes trust that they are the legitimate owner of an identity by using the biometric or other authentication mechanisms built into their phone. The phone is then used to scan a QR code displayed on a POS terminal or on a web page. Once the QR code has been scanned, the user's phone asks if they wish to proceed with a given action or to allow the web page access to their private data. If they consent, the terminal or web page can proceed with the action.

In this way, the identity token isn't limited to the device on which it is held; it can be used to enable access and activities on other devices and systems.

Privacy-Preserving Trust

Every identity has a unique name. Upon request (and, where required, upon payment of a fee), an external entity can ***attest*** to the fact that an identity with a given name has a particular property. For example, by submitting an image of a driver's license and verifying that the details on the license matches the other information associated with that identity, an external entity will attest to the fact that the identity has provided a valid driver's license. The fact that this identity has a valid driver's license is called an ***attestation***, while the details shown on the driver's license (including the photo, date of birth and full name) are ***personally identifiable information***, or PII. The attestation itself is public, while the PII is not.

Once the user has authenticated themselves to the satisfaction of a given third party, that third party can have confidence that the user has the properties defined by their identity's attestations. For example, they can be confident that the user has a valid driver's license, even though the license is not presented to the third party, simply by virtue of the fact that the identity has an attestation proving that they provided a valid driver's license. The actual license (and the PII it contains) does not need to be revealed before the user is given permission to do something (such as hire a car) which requires possession of a valid driver's license.

In this way, attestations provide a ***zero knowledge proof* —** that is, a way of answering questions about an individual without divulging personally identifiable data. On the basis of such proofs, third parties can, in good faith, authorize useful but risky actions such as purchasing an item or service, driving a car, voting, sharing medical records, and viewing restricted content.

Note that it is up to the third party themselves to decide what weight to put on a given attestation. For example, if a driver's license attestation is five years old, they may require an updated attestation before accepting it as proof that the user still has a current driver's license.

Identity Tokens in Today's World

In the brick and mortar world, users are already familiar with everyday authentication challenges such as door locks, key cards for access, and PIN codes on payment terminals. These are all simple forms of identity tokens which we use today.

In the virtual world, we are expected to either use siloed apps on a phone (for example, Facebook, Telegram or Snapchat), or else use a web browser running on a mobile device, laptop or desktop computer. Because legacy browsers are moored to the device rather than the identity, the traditional approach of using cookies to track usage has resulted in the worst outcome for everyone: the user regularly has their privacy violated through inappropriate tracking, while the operators of the site gain (at best) an imperfect idea of the user's identity as devices are often shared among more than one user.

If two different people share the same browser at home, the constructed identity gleaned by third party sites that are visited by those users will be a composite of those two people. Because there is no assurance that mere usage of a cookie-laden browser corresponds to any particular person, traditional browser sessions cannot be relied upon to securely grant permission to perform an action – be it ecommerce purchases without a complex checkout procedure, viewing age-sensitive material, or creating user accounts on a social network. In short, traditional browsers, even with cookies and password managers enabled, are at best imperfect foundations for granting permissions and, at worst, attack vectors for both privacy and security vulnerabilities that affect both individuals and society as a whole.

Baking Identity into the Browser

As an alternative to the current cookie-based approach to identity, identity tokens can be built into the browser itself. Using this approach, strong authentication, complete with privacy controls, becomes the baseline method for browser usage across the World Wide Web. To achieve this, a conforming browser would allow a user to scan a QR code with their phone at the start of a browser session, transferring their tokenized consent from their mobile phone to the browser. Once authenticated, the browser would display the user's name and picture to confirm an actively authenticated session. The site would know the globaliD name and any public information about the user, but no private PII would be revealed.

Once the user has authenticated, the site can programmatically ask zero-knowledge questions before granting access or permission to the user. These questions are answered by querying the public registry of attestations made against that user's identity, or by asking other zero-knowledge questions that include financial, location and other "facts" about that identity. The types of questions that can be answered include:

- Is this user over 18 years of age?
- Can this user spend $200 for this purchase?
- Is this user an accredited investor?
- Is this user a resident of an approved country for us to sell and ship to?

While the user maintains an active session, these questions can be answered immediately, without the user having to respond at all. Before a particular risky activity is being undertaken on a browser, the site may ask the user to reauthenticate themselves by displaying the QR code again. Other multi-factor and multi-sig challenges are also available. Note that when the app or web site is running on a mobile device, the QR code cannot be scanned because a tokenized phone cannot scan a QR code displayed on its own screen; in this case, the user can be prompted to enter a PIN code or perform a thumbprint or face ID to authenticate themselves directly on the device.

When the user leaves the browser, they may or may not close the browser window. If the window is closed, there is no issue as the session is automatically terminated. However, for desktop browsers, there is the risk that the user may leave the window open and simply walk away. In this case, the user's identity may still be connected to the browser, leading to the possibility of another user sitting down and accessing content and ecommerce sites without having to authenticate themselves first, leading to the risk of unauthorised access and fraud. A number of things can be done to mitigate this risk, such as requiring the user to reauthenticate themselves after a given period of time. A more clever solution to this involves comparing the user's phone's current location with the location of the phone at the time the user scanned a QR code on that phone. Assuming a fixed desktop computer, any variance is an indication that the user has moved away from the computer[1]. Another possible approach would be to use Bluetooth to check that the user's device is still physically close to the computer running the browser.

[1] This won't work if the user is running on a laptop in a moving vehicle, but the overall pattern of usage compared with ongoing location of their phone can give an indication of this. At worst, the user might be asked to re-authenticate themselves more often than they would be if they weren't moving, but this doesn't prevent them from having an authenticated session and using their identity token to perform actions and access information that requires them to be authenticated.

A Better Web Experience

By enabling secure identity tokens and zero knowledge proof at the browser level, several existing tenets of the how the web works today are called into question:

- The cookie-laden browser experience commonly associated with Safari, Chrome, and Internet Explorer is unnecessary. The use of a transferred identity token would, for example, allow the user to make micropayments in exchange for expeditious ad-free browsing. Alternatively, a user might can gain access to content by consenting to a requested action, such as viewing an advertisement, sharing an identity attribute, or taking a survey. Existing browsers lack the level of authentication required to perform these types of actions in a privacy-preserving but trusted and secure manner.

- Instead of sharing personally identifiable information to third parties in the way currently done by sites such as Facebook, it will be possible to provide zero-knowledge answers to questions without revealing the user's PII. Even when Facebook credentials are presented for opening accounts and posting content, the identities behind such actions and content can be cross checked as either globaliD authenticated (more likely to be true) or unauthenticated (possibly more likely to be fake).

- The Amazon-like one-click model can be extended beyond the Amazon silo. This will allow all content and ecommerce sites to accept browser-authenticated payments and shipping details. Because the tokenized browser itself carries payment and shipping details associated with an authenticated name, there is no need for a payor or payee to rely upon a centralized repository such as Amazon for such details.

- The iOS versus Android duopoly continues to play out as a game of market share between competing rather than complimentary solutions for identity. For them, gaining market share and margin has, to date, been more important than working together at the protocol level. Competition has prevented these mobile operating systems from rising to a protocol rather than mere platform level. The same can said of competing messaging standards. For example, WhatsApp, WeChat and iMessage users are trapped into individual silos rather than able to cross-communicate (or more importantly cross authenticate). Biometric and OAuth2 like solutions work for siloed authentication but do not allow mobile operating systems or messaging stacks to interoperate across the web, leading to segregated user bases. Telecom-based SMS is universal but is not powerful enough to build authenticated rather than merely routable identities.

- Visa, Mastercard and traditional banking systems may still be used to make payments, but since every globaliD-named entity – be they a user, content provider or ecommerce provider – has a “hot wallet” that can hold any store of value, the parties can directly settle any micro or traditional payment without reliance on card or bank payment rails. Card networks do understand tokenization well, but they tie it to their siloed systems rather than working at a broader level – especially one that may separate their slowly and costly clearing and settlement functions from their actually quite robust and scalable tokenization efforts.

- Media giants such as the New York Times and Wall Street Journal currently require a subscription to access content. This crude model can be replaced (or supplemented) by a pay-as-you-go micropayments scheme, where users essentially have a tab that allows them to access broad swathes of web content.

- At present, access to content and activities that are restricted, regulated or licensed is implemented on a site-by-site basis, if at all. Anonymized sites such as Craigslist are notorious for fraud, abuse and worse. Through the use of identity tokens and zero-knowledge-based permissions, a secure and effective rating system for violence-, sex- and age-related materials and activities can be built directly into the browser. This allows the browser itself to provide privacy-preserving safeguards while dramatically reducing the occurrence of scams, coercion, and fencing of stolen goods.

A New World

Tokenized identity built on top of a self-sovereign identity namespace will directly challenge existing business models, both in the brick and mortar world and on the web.

While change happens relatively slowly in the brick and mortar world, the sweeping reach of the World Wide Web suggests that transformation will occur there much more rapidly — especially if this is enabled at the fundamental level of the browser. Granted, content and e-commerce providers still need to accept browser-authenticated identity, payment, and shipping details, but there are compelling privacy, security, economic, efficiency, and UI/UX benefits to doing so. The user benefit of being securely but privately authorized via tokenization is even more clear cut.

Cookies, passwords, and all the privacy compromises, hacks, theft, fraud, fake identities, and fake news that go with the status quo are now clearly avoidable in a *practical* manner when authentication is based on identity tokenization built on top of the globaliD namespace. The status quo approach of based security on something we know is a nothing more than a security-by-obscurity expedient. Unfortunately, "something we know" all too often becomes “something all too many others know as well.” By using something we have rather than something we know, identity tokens make it easier to be good than bad. Maintaining and using a good tokenized reputation is far easier than trying to ensure that bad actions taken and associated with a particular name do not make it reputationally unusable.   While a bad actor can always start over, choosing a new name and creating a new identity from scratch, the lack of a reputation for a name is itself a searing red flag that will force the bad actor to spend significant time and effort to build up their new identity. This makes the creation of trusted but fake identities a challenging and time-consuming ordeal.

While "ease of being good" through tokenized authentication in the brick and mortar and virtual worlds may not sound like a terribly high aspiration, it is eminently achievable and transparent, and is a sound foundation to build on over time.   And while many others already sing the praises of tokenization, it seems that most if not all consider identity tokens to involve the sharing of private credentials like a phone number or social security number, rather than universal public credentials such as a globaliD name backed up by zero-knowledge-based permissions. Just as the domain name system (DNS) made the web ubiquitous in a way that AOL and Compuserve could never match, identity tokens and the globaliD Identity Namespace System (INS) have the potential to make secure and trusted yet privacy-preserving identities ubiquitous in both the brick and mortar and the virtual world.

What matters is far less the particulars of any given technology, but rather the move towards an objective authentication/authorization model that is independent of any particular actor. Without this, the promise of the web, just like the promise of free speech, is diluted by the “identified” but unauthenticated fraudsters, fakes, and trolls – tipping the scales in favor of proverbial bad apples that spoil the barrel.