SiriusID
Powered by ProximaX

SELF-SOVEREIGN ID

Contents

Self-Sovereign ID

1. Introduction

The idea of a digital identity has been around for more than 30 years. The absence of a proper global solution was the stumbling block to how this could be implemented. Privacy, security, data persistence, accessibility, and ubiquity of such data were among the main issues. When Internet was more pervasive, some of these problems could be solved but the others remained largely unsolved. Designs such as the ability to locate an ID based on the concept of a domain name, an email address, an IPV6 address, commercial PKI infrastructures, and url could not possibly solve the issue because these names are usually on lease or not easy to obtain via a central registrar. This transient nature of the lease, commercial viability, and inaccessibility of such services makes it hard to implement the solution on a global scale. Blockchain technology purports to solve most of these issues and is the best candidate to implement this on a global scale with interoperability, like Internet.

Consequently, the concept of a domain name gives rise to an idea that could possibly be borrowed and adapted for blockchain networks. First and foremost, it allows for the creation of an ID that is rooted into the blockchain, thereby allowing us to have persistency in an ID.

Early designs were based on a digital ID sitting in a central database, a standard procedure. Each of these databases carries a hash table. The design morphed over time by the creation of decentralized hash tables (DHT) that can be referred to. However, this type of solution was not so scalable and reliable as they were being linked to an email which was transient. DHTs are basically a central store of all digital IDs issued by an operator, where each entry is a unique identifier consisting of a string of characters. It does not have any meaning other than to record the existence of an identity belonging to an individual, an organization or a thing - like a mobile phone or a car. This hash points to the owner of an ID which could be tagged to an email. The use of cryptography science ensures that the entry belongs to one single person which can be verified. This method of DHT that is disparate in existence, uncoordinated, and lacking in data persistence makes it hard to uniformly implement globally. Further, the security measures that need to be put in, the potential loss of data through inadvertent deletion, and accessibility posed great challenges.

Blockchain technology allows for persistence of data, and combined with cryptography science, peer-to-peer technology, it appears that this solution is the most apt solution for digital identity.

The concept of a digital identity should allow for one's self-sovereignty over the ID. There are a few elements that we need to be familiar with before one can grasp the idea. The elements of this very simple concept are:

1. Credential or a trusted issuer
2. Decentralized Identifier – DID – a universally addressable URI-based identifier provided by a credential issuer.
3. DID document – a digital certificate signed, and issued by the credential issuer. It usually comes with a hash of the digital document. A hash in simple terms, is a long string of characters that represents a digital thumb-print and is unique to each document.
4. Credential Inspector, also known as the entity requesting the credential for processing, e.g., a bank requiring your ID.
5. A master ID or Self-Sovereign ID (SSI) – an ID that could be used by a person as the owner of all the DIDs that are issued by all credentials. Liken it to an ID given to a physical folder that holds all your material credential certificates issued by various authorities or trusted institutions, or "that black oblong shaped physical leather wallet holding a bunch of cards issued by various entities."

1.1. Credential issuer

A credential issuer can be an individual, an entity or institution or a government body. It does not matter who issues it, and whether it is a trusted source or not. It depends on how the credential inspector will want to trust or accept the credential issuer.

1.2. Decentralized Identifier (DID)

It is a unique identifier given by a credential issuer to the person/object seeking for such a credential. It can be likened to a unique serial number given to an entity, be it an organization, an individual, or an object. W3C has standardized a DID to look like this:

did:Prx:6HA785421EBC74562891I85TW847DOP19F

It is broken into 3 parts, separated by a colon. The first part is the scheme, which is the W3C proposed scheme and is fixed. The second part is the DID method, which is the organization or technology network providing the DID. The third part is the DID method specific string. It could be a hash string of the document, or it could be a message string or just an ID, and is unique.

This DID, if the standard is followed, can be looked up from the internet. It is a Uniform Resource Identifier (URI) for the DID.

1.3. DID document

It can be issued to a person, an organization or an object of reference. The credentials issued could be a government issued identification such as a passport, an national ID, a university degree, bank credit rating, land, car, mobile phone, tree, plant, and animals. In short it is a digital document with a signature issued to anything and by anyone, trusted or not.

1.4. Credential Inspector or Verifier

A credential inspector is an individual, an inspector or an organization, who will be making use of the decentralized identifier document to process and verify the existence or credibility of the DID holder.

1.5. W3C[1] – Standard for DID

When blockchain came into existence, it was not until around 2016 that work seriously got started on establishing a standard at the W3C. Its objective was to develop a standard for global acceptance on decentralized digital identity so that this standard, if adopted, gives rise to the ability to produce a digital identity anywhere, anytime, and with trust from any credential issuer. More importantly, it allows for a standard method for addressing and referencing DIDs across all platforms that comply with this standard.

This method of standardization which is platform agnostic, provides a fair means for all those working on digital identity solutions the ability to work across all platforms that conform to the standard. Additionally, it allows for widespread adoption and allows users to

[1] The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web.

transparently use their DIDs anywhere, anytime, independent of the provider, so long that these providers conform to the DID standard.

1.6. ProximaX SiriusID – Putting it all together

The ProximaX SiriusID solution is conformant to the DID method. ProximaX has developed an SDK and plugin which allows any provider to easily create their own DID solution. Additionally, our platform allows anyone to create their SiriusID ahead of signing up with a provider.

SiriusID is an identifier that can persist in our network. It is a super identifier that overlays onto the DID as proposed by the W3C working group such that every DID document that is issued by a credential issuer can now be owned by the holder of a SiriusID with persistence and ownership, vis-à-vis an email, which is not.

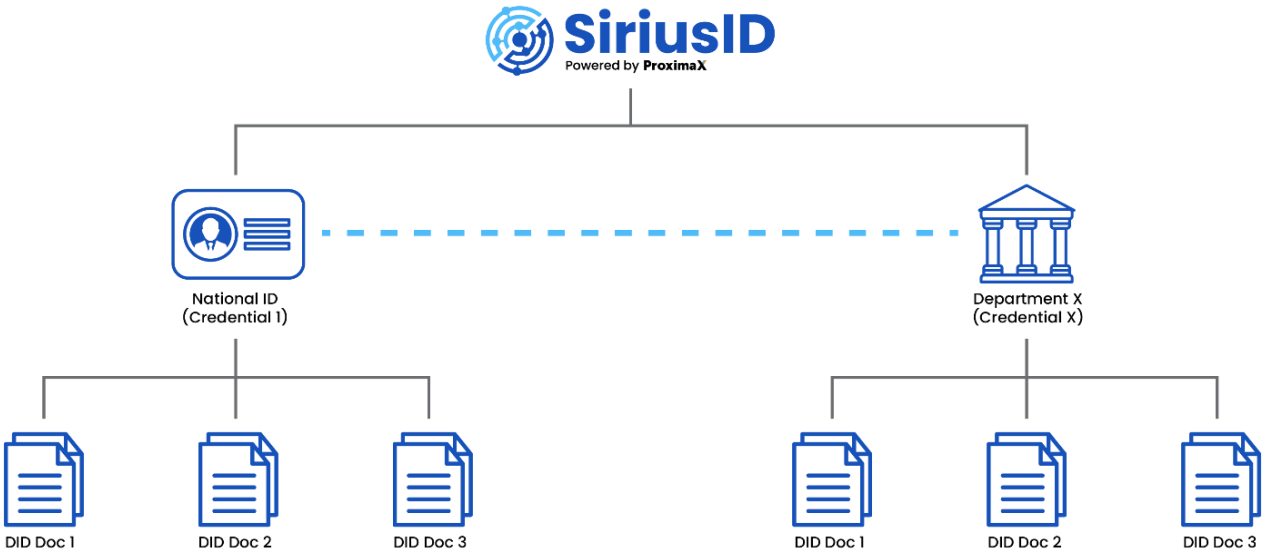

Figure 1. A SiriusID can own multiple DIDs issued by multiple credential sources

SiriusID can be rooted in the ProximaX Sirius public network, or if need be in a ProximaX Sirius private network, or a hybrid of both networks.

SiriusID enables any individual, entity, or subject to be identified with a digital signature and an association. This SiriusID can be used for DIDs issued by credential issuers so that multiple

DIDs from multiple credential issuers can be issued to this one entity owning the SiriusID. The more DIDs it has, the more verified this SiriusID is and therefore the credibility associated with it.

A DID is a unique identifier that is issued by a single provider for a single entity. It may contain many DID documents issued. An example of a National ID (the physical ID) with a DID given to a person with three DID documents could be:

1. A DID document with picture profile of the person and name of the person (two of many fields extracted).
2. A DID document with picture profile, name and national ID number of the person (3 of many fields extracted).
3. A DID document with all the details associated with the person (all fields extracted).

All the above bear parts of the entire National ID of the person. Depending on its use, this person can selectively give a verifier a document sufficient for its purpose. If the person decides that a verifier should only need to know the picture profile and the name, then document one is enough. The document can be verified with the credential issuer – the national ID registration body – which is a trusted body, and therefore does not need to verify more about the identity of the person as this person exists.

There are many more ways of verifying a credential, including the use of ProximaX Sirius Supercontract where predefined logic and rules can be implemented.

The SiriusID platform provides for a distributed storage of DID documents. Credential issuers can store these DID documents either on their own distributed storage network, or on the distributed public storage network. The solution is highly versatile and allows for a few different types of configurations. Persistence is optional and is dependent on whether DID documents have an expiry date or not. In many jurisdictions, it may be required that these DID documents be removed totally after a certain period of time or by the DID owner.

The use of Supercontract and storage makes the SiriusID a very powerful and complete solution for the implementation of digital ID. The SiriusID is the only platform that currently exists, which provides an all-in-one solution incorporating storage, blockchain for ID and hash persistence, and Supercontract. The solution sits entirely in a tightly integrated platform and comes with a complete set of SDK and APIs to allow for easy development of an identity application solution.

2. Use Cases

The use of a SiriusID is suitable for most situations requiring some form of identity. These could include:

- Private and public access – buildings/facilities/carparks
- Financial institutions - Credit rating/AML/KYC
- National ID/passport/citizenship/birth certificate/driver's license/marriage registration/Tax ID
- Title registrations – vehicle/property/pets/securities/company registration
- Utility registration – electricity/mobile phones/gas/water/Internet access
- Health care – medication/hospitalization/health records
- 2FA authentication and website/application logins
- Document signing – agreements/contracts/notarization
- Proof of origin – provenance/patent/equipment manufacture/drugs
- Certifications
- Voting – election/local council/company
- Smart city implementation
- IoT
- Payment

The use cases are numerous. It has not been possible previously, and with the advent of blockchain technology, suddenly a whole new paradigm comes into existence. There was no efficient way to verify identity.

As a complete platform, the ProximaX SiriusID allows for any organization to quickly deploy their solution in a very short time. There is no need to set up individual components to complement the entire set up. These individual components may include having to develop and integrating into a blockchain platform, incorporate a database, and then develop a storage system to be integrated into the overall system. Security and network planning are also needed when disparate systems are put together. This could take up a lot of time and resources.

The SiriusID platform has all these components put together and abstracted in the form of SDKs and APIs, allowing the developer to easily implement the system without knowing

much about the blockchain and storage technology. By default, all documents stored are encrypted and sharded into multiple pieces of information, with each piece of information itself being encrypted.

The following use cases shows how the SiriusID can be implemented in a short period of time.

2.1. Government issued identities

Many countries have their identities issued and managed by multiple agencies. For example, the immigration department looks after the issuance of passports, while the road transport authority looks after the issuance of a driver's license. Additionally, birth, death, marriage certificates, citizenship, and national identity may be issued by yet another department. Usually they work in their own silos. To get a passport, one has to produce an identity that is recognized. This could either be a citizenship certificate or a national ID.

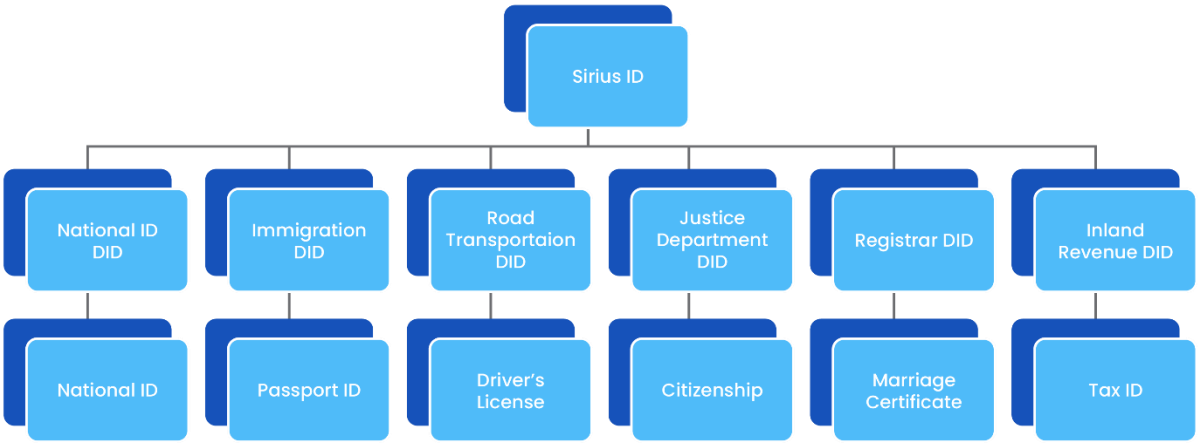

Figure 2. Each department to issue a DID and attached to the SiriusID for foolproof credential

There have been many reports on how documents can be fraudulently issued in third world countries. Since departments don't necessarily coordinate with one another, physical sighting and validation of an identity document in most times, is sufficient to issue a passport. With this loophole, insiders in the immigration department can fraudulently issue a passport, bypassing sighting of any other identity documents. As a result, passports are

issued indiscriminately to illegal aliens resulting in human trafficking and other illegal activities.

In order to address this problem, a SiriusID can be used to solve it. As shown in Figure 2, every DID issued by any department must have a SiriusID attached to the DID. Each of these DID documents issued must bear the same SiriusID and a department specific DID so that the credential of the holder of any of these documents can be verified.

Each person can then generate her own verifiable DID documents with the SiriusID and DID issued by these departments.

With a common SiriusID and specific DIDs issued by each of these departments, it is then not easy to cheat the system. In order to cheat, entire systems must be compromised. It will involve a large syndicate to do so.

For example, if the immigration department is fraudulent, it will have a SiriusID different from that of the national ID department who may most probably be different. The same applies with the driver's license, or marriage certificate.

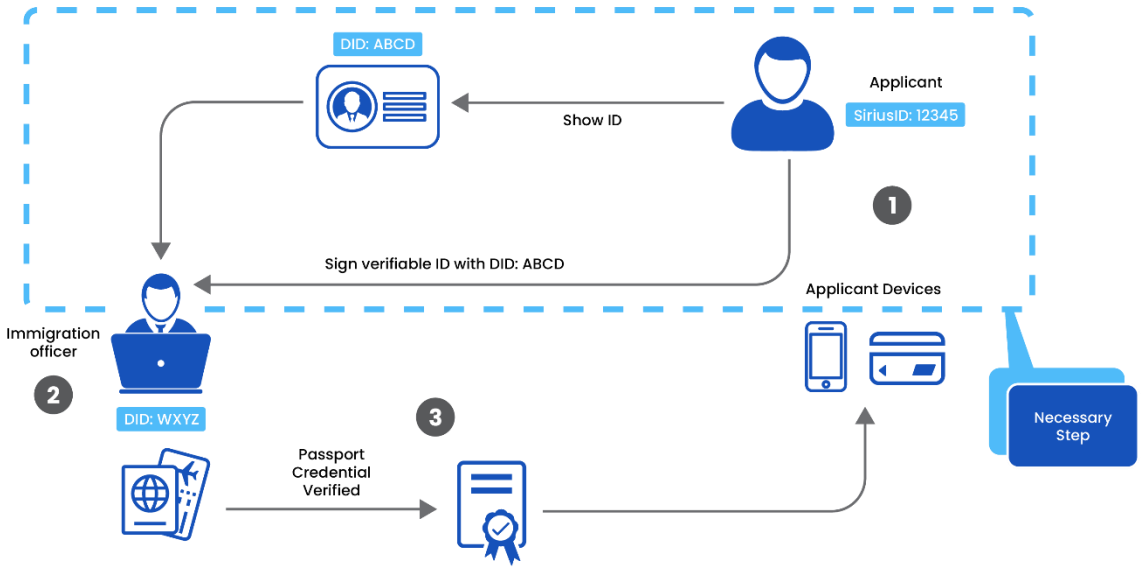

Figure 3. One proposed procedure for the issuance of a passport.

In most countries, the first stop is to get a national ID. A citizen can usually obtain a national ID by producing her birth certificate or citizenship certificate. A national ID is then issued to

this person together with a SiriusID and a department specific DID which is tagged to the national ID.

Figure 3 shows a possible method to apply for a passport. A citizen walks into the immigration office, presents an identity - a citizenship certificate, or a national identity - together with other supporting credentials such as the driver's license, birth certificate, all tagged and signed by the SiriusID.

Once signed, the immigration can verify the DID documents to ascertain the identity of the person. Thereafter, the office proceeds to issue a physical passport, including issuing a DID that is tagged to the SiriusID for the citizen, following the same onboarding procedure as the other departments in issuing their DIDs.

Once a passport is issued, the citizen now has another ID credential to her name.

With the use of SiriusID and a national ID, it is then hard to fraudulently issue a passport. Even if it is issued, the border control can easily fish out the SiriusID of the passport holder and get the person's details, including the DID of the national ID. Failure to extract the national ID through the DID results in the passport holder being marked as a potential illegal alien.

2.2. Verification of an inbound passport holder

Most countries are becoming more electronic in their processing of inbound visitors. For inbound citizens, where there is an electronic gate border control, this solution can be built into the system by calling up the DID of the national ID of the person to verify, including matching their photos with the actual face of the person at the electronic gate through a facial recognition solution.

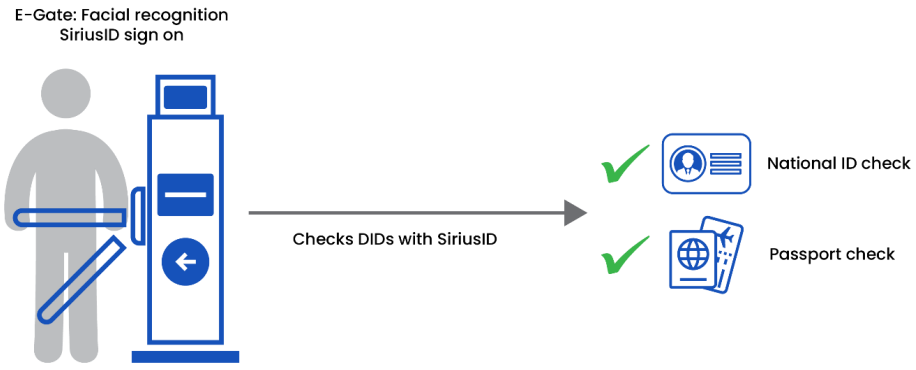

Figure 4. Performing multiple checks to verify inbound citizens

Circumvention becomes very difficult other than smuggling them into the country. In other countries, if they have implemented a compliant DID, immigration officers can also ascertain a person by checking the DID which can be verified following the W3C standard.

Increasingly, syndicates are getting more sophisticated to cheat immigration systems. Apart from physically entering the country illegally, the implementation of a SiriusID solution can make the system more foolproof. Additionally, it can also make the entire ecosystem of identity management more efficient, thus harmonizing these identities across all government departments and agencies giving governments a more transparent access to identities of their citizens.

2.3. Single Key sign on

Imagine having to remember tens of passwords and losing them. Why not just one password that can be used for all? Here are the inherent problems associated with passwords:

- They are stored in the database of a service provider
- Passwords can be too easy to guess or compute
- It is rather hard to maintain a good password as it is hard to remember or too time consuming to key in.
- Passwords are often forgotten or misplaced, which makes it hard to upkeep.
- Passwords can be stolen from a provider and be used against the user to crack other services which may bear the same name and possibly same password.
- Storing passwords in a database subjects the provider to theft and hacks.

Centralized control of passwords is one of the biggest challenges of today. Too many times, too many service providers are reporting loss of passwords and user data to hackers and thieves. It needs a total re-addressing. This has not been simpler until today where we can make use of cryptography that is more accessible and developed for everyone to use. The SiriusID is one such solution where it can be used to sign on to a service.

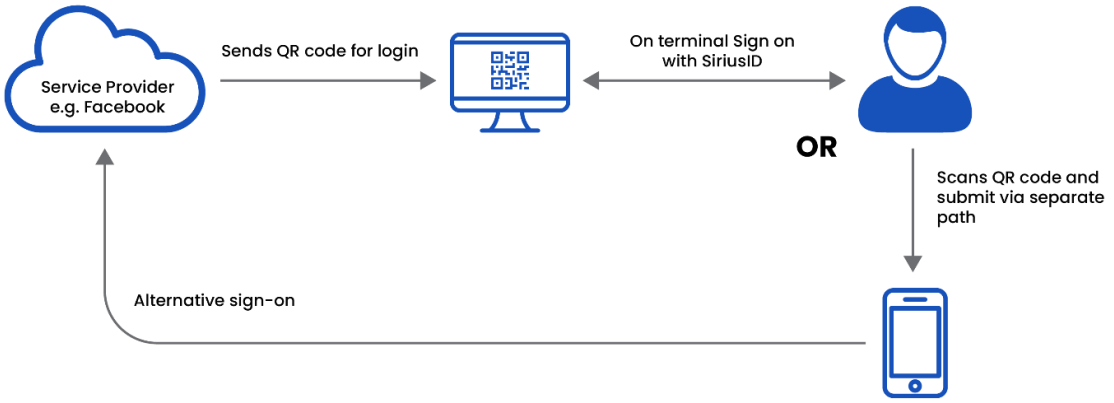

Figure 5. A simple login process using SiriusID

Figure 5 shows how a login process can take place. Firstly, there is no password required or stored on the side of the service provider.

Secondly, in order to register with a provider, the user needs to provide only the public key of her SiriusID to the provider. This public key is stored in the provider system to be used to reference the ID of the user.

Thirdly, to sign up as a user, the user can choose to use a verifiable DID so that the provider can then verify the user. This option of course limits the provider from the ability to learn more about the user, thus giving the user more privacy. In the long run, it is expected that new laws are passed to ensure protection of privacy of users by way of DIDs.

There are many ways to implement the SiriusID solution from the provider side. It all depends on the level of control. Traditionally, the more control the provider has, the more centralized the solution is and therefore the more vulnerable the system will be. At the other end of the spectrum, having no control, the responsibility is passed entirely back to the user. Losing a SiriusID could mean losing everything. The SiriusID can work across this spectrum of control.

2.4. 2-Factor Authentication (2FA)

Often, in order to increase login security, the SiriusID can be further extended to be used as a single key 2FA sign-on for all services. Again the spectrum of control depends on how a provider implements its solution.

3. Deployment

The solution is an all in one platform. What needs to be done is the frontend that is required to integrate with the SiriusID. The solution comes with SDKs and APIs for easy onboarding. A typical system can be implemented within two months from a bespoke build.

If there is a need to integrate with existing systems, it will depend on how the entire solution is to be mapped out to include digital ID. This usually requires a detailed study on the various actors in the ecosystem, their roles and their requirements.

The ProximaX solution is a holistic platform and is the most full featured solution in the market when it comes to flexibility, design, and development.

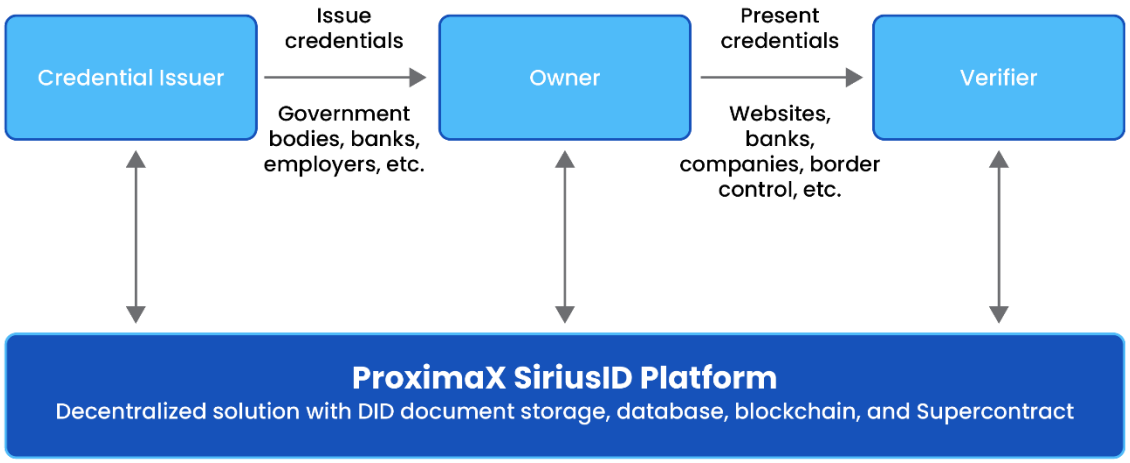

Figure 6. ProximaX SiriusID platform for deployment

As can be seen in Figure 6, the SiriusID platform is a "monolithic" cluster of distributed servers located across the Internet or a VPN. Each actor interacts with the platform and perform various tasks. The credential issuer uses it to store information and create DIDs. The owner uses it to update and manage DID documents. The verifier uses it to verify DIDs and DID documents.

The design is simple and neat and requires little integration other than integrating with existing systems if there is already a legacy solution. Porting over digital information from

legacy systems does not really require a lot of revamping and could be ported over by exporting user data and tagging a DID to it upon export.

4. SiriusID App

To showcase how simple it is to build on the SiriusID platform, ProximaX has developed and integrated an SSI app named SiriusID that is available as a white-label product.

With this app, users can generate a SiriusID and collect credentials.

Credential issuers can tag credentials to SiriusIDs.

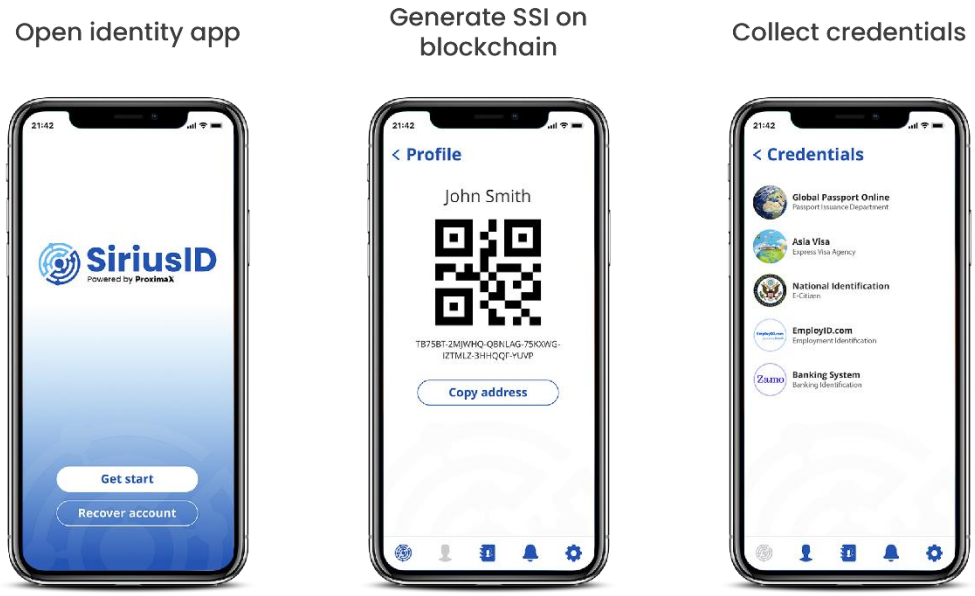

Figure 7. SiriusID app identity management

Credential verifiers can verify credentials.

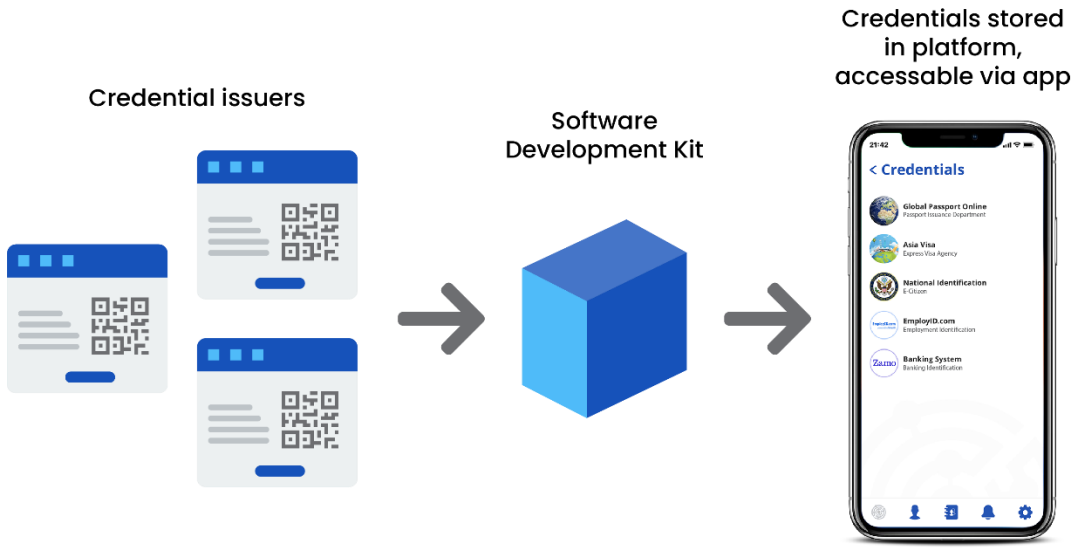

Figure 8. SiriusID app credentials creation

Real world scenarios can be showcased such as passport issuance and verification.

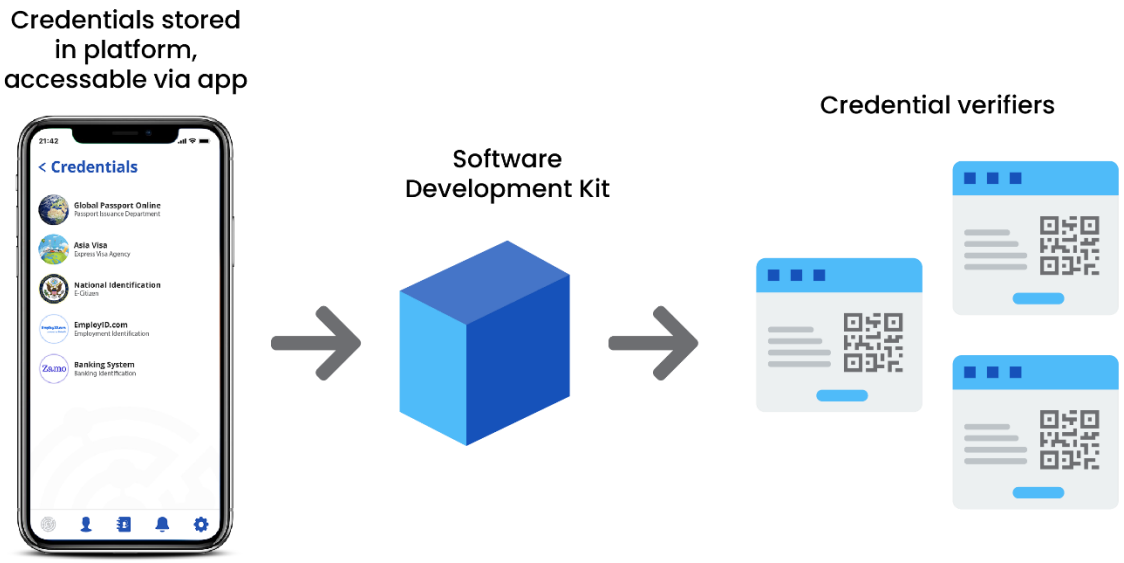

Figure 9. SiriusID app credentials verification

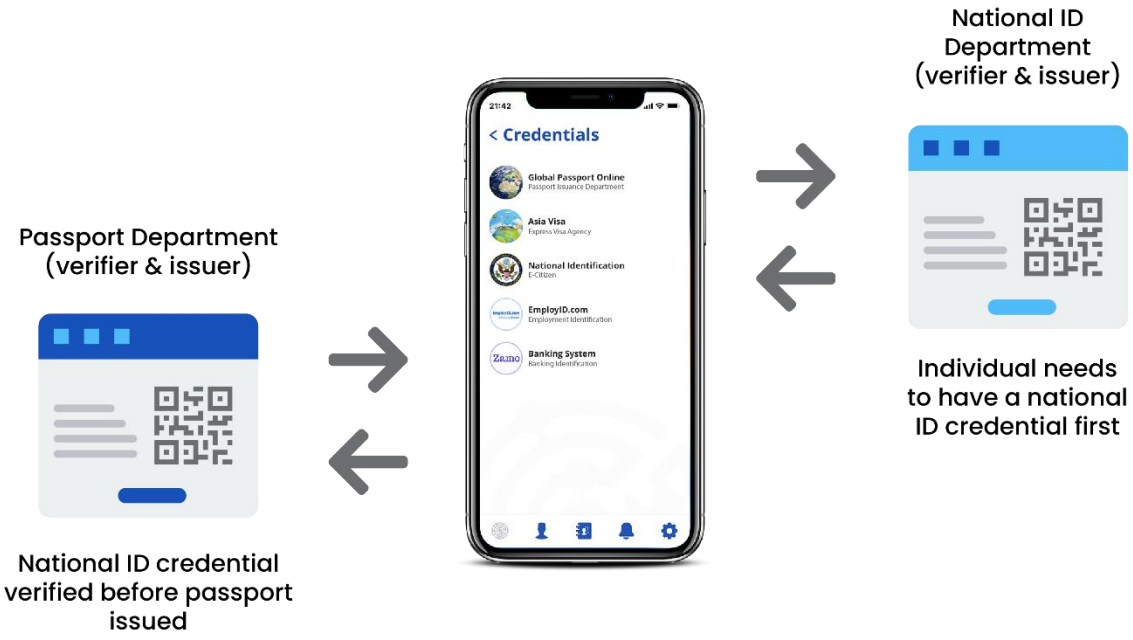

Figure 10. SiriusID app use-case - passports

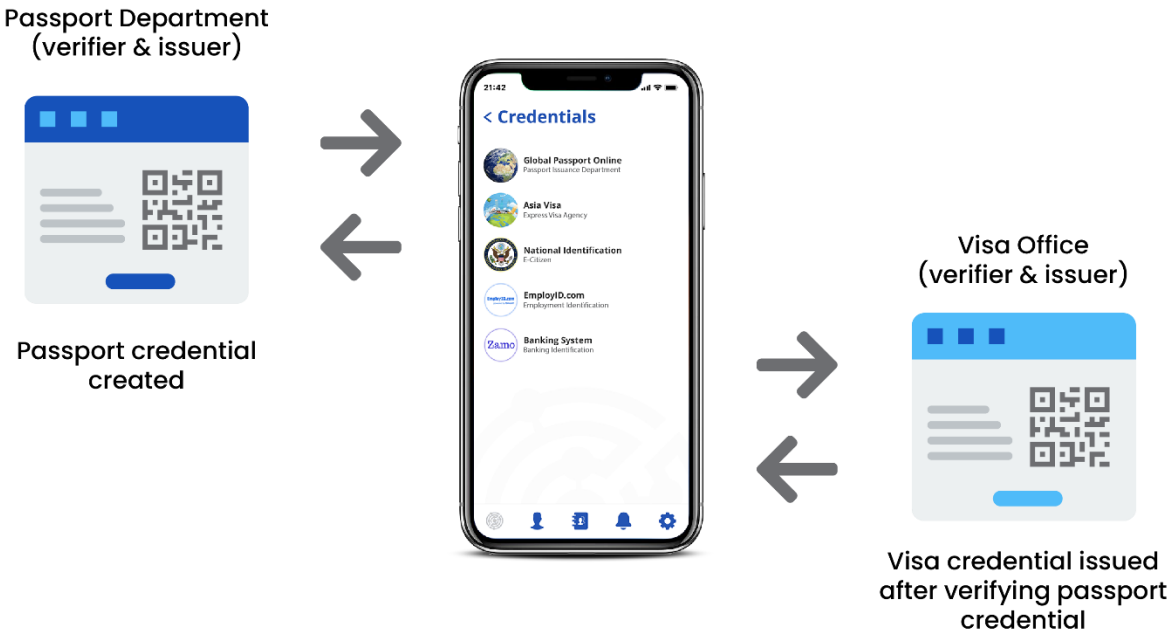

Figure 11. SiriusID app use case - visas

A user can also access services and secure environments using a single key sign-on.

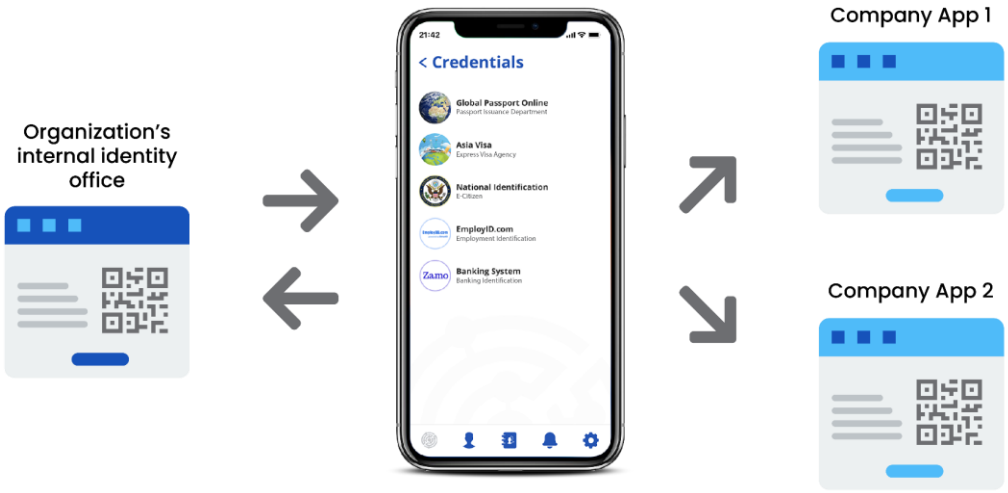

Figure 12. SiriusID app single key sign-on

5. Moving Forward

We have seen how Self-Sovereign Identity has evolved in the last thirty odd years. It was not until the advent of blockchain technology that it brought about harmonization and standardization on a global scale.

ProximaX's SiriusID solution has given us a very powerful option that can be adopted and used by any entity. Most of all, it complies with W3C and is enhanced in that credential issuers can also issue DID documents in a distributed and permissioned manner on the SiriusID.

The SiriusID solution is extended to include the possibility of even selecting fields into creating one's own DID document, so long that these fields are verified originally by the credential issuer. The solution will come with SDK and APIs so that system integrators can develop their applications in a single infrastructure platform without needing to integrate other components to complete their applications. This not only cuts down the time-to-market, but also the learning curve required to develop an SSI solution.