Hyperledger Identity WG

[See volunteer doc](https://docs.google.com/document/d/1zDPVDer9G-IjqicB65G9Uo2RhzpYLY4mGpVpEPu_Wt4/edit?usp=sharing)

**Procedure for volunteering:**

Ideally the part that you volunteer for should be doable in an afternoon (about 200 to 300 words) and should be a subject that you know something about, or are willing to research from a variety of good sources. Please put yourself in as a volunteer in the sections which need volunteers and put a tentative end-date. We need references used to create your material.

**~~People with links can comment, but not edit the document.~~**

**I have thrown open the document for editing. Please be respectful of others’ contributions. Do not add irrelevant material. Insert comments or suggestions if unsure and we will incorporate into the document.**

# Introduction

The aim of this document is to model the concept of Digital Identity as it applies to Blockchains and to the DLTs in Hyperledger in particular. It is **not** to come up with watertight definitions of the concepts, nor discuss philosophical implications regarding Identity, nor discuss digital Identity in the context of generic digital Interactions on the Internet as many others have done so more elegantly[[1](#8na79d6l0uug)]. The functional definition of Identity: “Identity is how we keep track of people and things and, in turn, how they keep track of us” is one of the principles under which we model Identity in this document, recognizing that Digital Identity and its modeling is just one of the subsets of the topic of Identity.

The main purpose of the paper is to aggregate the collective wisdom around Identity and Blockchains, focusing on the DLTs hosted by Hyperledger and cross-cutting concerns. As the topic is vast, the concepts are presented at a fairly high level with a list of references. Anyone who is interested in identity and Blockchains has the opportunity to drill down with the references into deeper readings. We examine the role of Identity in Interoperability in the DLTs around Hyperledger as well as explore ways to bridge between these and Legacy systems. The ideal reader of this paper is a person who is interested in Digital Identity on Blockchains without specialist knowledge on DLTs nor Identity. In this paper we also describe the current state of the art in the projects in the Hyperledger hothouse and how they solve the problems posed in the use cases.

The use of DLTs provides a unique opportunity to wire identity at an architecture level. Now we can envision a systems built with Self-sovereign Identity (SSI) and Distributed Identity (DID). Many DLT initiatives have started to create such a solution for Identity. They also seek to wire a seamless transition from legacy systems implemented mostly using PKI to the new world of SSI. We will look into some of these systems later. Below are some high-level real-world problems that DLT-based identity can address.

1. Proliferation of username-passwords  
   In today’s internet, identity is centralized and is controlled by each and every domain. As a result, a typical person has 50-100 username-password pairs.
2. Insecure passwords  
   Today’s identities are mostly authenticated through passwords. However, passwords are insecure. A password-based system that is easy to use is prone to social and other technical attacks.
3. System-controlled Identity  
   Today Identity is system dependent. Whether it is consumer facing (B2C) or business facing (B2B), each create their own identity database. Data migration becomes a difficult task and usually at the mercy of the system. A regulatory framework like GDPR tries to force companies to address data privacy, data portability is addressed by GDPR as well and PSD2 in Europe, however Identity portability standards are still evolving.
4. Data Breach  
   These identity databases also create the treasure trove problem. As username/passwords are stored in centralized systems, they create great incentives for hackers to get a hold of the database. If you follow all the high profile data breach incidents, you notice a trend of hackers going after more and more concentrated databases. From the Target hack to the Yahoo hack and the Equifax hack, more and more accounts are get affected. Even more alarming is the fact that the general public have data breach fatigue and care less and less about protecting their personally identifiable information(PII).
5. Legacy system interoperability

As noted before, when applying DLTs to the enterprise, one has to address the issue of technical debt. Most enterprise systems run on centralized identity systems such as LDAP or Active Directory. Bridging the gap between legacy identity providers and DLT-based identity system is a necessity.

1. Real-world Digital Identity

If you are reading this white-paper, chances are you have a government issued identity. However, more than one billion people in the world do not have one. As a result, they live outside of global support and the global financial system.

In a second and more technical paper we hope to present an Identity Interface definition for an Digital Identity Utility and propose a path toward an implementation in the context of its use in DLTs under the Hyperledger Umbrella and beyond. In order to make Interoperability practical we will propose an Interface to the lifecycle of Identity as well as to create an implementation project for a thin layer around a Identity library for use inside any Blockchain implementation to manage lifecycle, and to use the Identity library to interoperate. We may use an existing library like Indy to be the basis for such an implementation.

# Core Concepts

An Identity can be modeled as a dynamic collection of claims attached to an entity, usually called a *subject*. ‘Attaching' could happen, for instance, by means of a string that is referred to by many names, e.g. 'subject', 'identifier', 'identity', 'primary key', 'DID', which functions as a unique identifier or a key. As new data comes in or new ways of interpretation of old data come about; this may be used to modify or create new attributes; hence the word “dynamic” is used. In order to accrete trust and be useful for authorization, these attributes must be verifiably attested by other entities, called *issuers*. A *relying party* relies on the attestations to engage in a relationship with the subject with the proven Identity. A subject can have different Identities in different contexts, this multiplicity may not be evident to the relying parties nor the attesting parties. Each such view is referred to as a *persona*. There may be occasion to prove the equivalence of two personas of an Identity. If this happens inadvertently, and not as intended by the subject, this can lead to linkability and the loss of privacy.

Identity is a foundational concept in blockchains. A notion of identity has to exist before any transaction can take place on a DLT. Identity is needed to model Rights & Obligations.

Identity is tied to a set of attributes, like:

1. Assertions or Claims , “Name: Ken Casey, Drivers License NY: B1654289”
2. Attestations “DMV NY says Ken Casey has drivers license B1654289”- signed by DMV NYs private key
3. Assertion & attestation rolled into one. (BTC transfer resulting in new state of UTXO)

In an example of the simplest case, Identity can be publicly exposed as just a public key. In order to reduce linkability or side-channel attacks, these public keys may be for a one time use as long as the private key is used to prove the ownership of the identifier; for example as. In general, there is a private key which is a secret possessed by the entity controlling the identity. This private, public attribute structure is quite common, even for Identities attested to by Certificate Authorities. See PKI later in the document for details.

<diagram from Jason Law with three dimensions>

# Domains of Identity

As examine Digital Identity and the problems around Personally Identifiable Information (PII) held in data stores including blockchains, it helps to clarify the context in which the interaction and storage happens. Domains of Identity as defined by Kaliya Young[ ] can help us categorize these contexts in the use cases, standards and implementations cited below. This classification can help us be clear-headed about the scope of the solution and the questions to be asked. The following are the contexts in which the domains operate. In addition there is the context of the self and delegated self and of data brokers and data pirates. These are further broken down into the domains of Registration, Transactions and Surveillance.

* Government
* Civil Society
* Commercial
* Employment

This results in 16 domains enumerated below

• Me and My Identity

• You and My Identity (Delegated Relationships)

• Government Registration • Government Transactions • Government Surveillance

• Civil Society Registration • Civil Society Transactions • Civil Society Surveillance

• Commercial Registration • Commercial Transactions • Commercial Surveillance

• Employment Registration • Employment Transactions • Employment Surveillance

• Data Broker Industry

• Black Market

Kaliya’s paper is quite extensive going into the details of the domains.

Where relevant, we will call out the domains in the sections below. This helps us be aware of the context and the domain so that we can think clearly of the solution.

# Use Cases & Scenarios

[Reliability Ranking Schema](https://docs.google.com/document/d/1ffoVycbd0ZZCd0FeOrYSb1QRtLUQ9QMsQY0bZ0_TJEY/edit):

This is a simple way of evaluating the use cases in terms of the Reliability and Complexity. A three level ranking scheme that could be used in the analysis of use cases. Most of the use cases presented above are in the complex category.

1. Complex / Reliable (B2C, B2B and B2G use cases)
   1. Thoroughly tested and production-ready in a setting that requires:
      1. “protection of PII, information, regulatory scrutiny or pulling data from external sources”
2. Business Functional (B2C and B2B use cases)
   1. Run behind firewalls
   2. Only utilize internal data
3. Stable (some B2C use cases)
   1. Requires little complexity
   2. Breaches have limited implications

There are many potential ways to utilize identifiers on the blockchain. Many projects have proposed standards, regulations and specific applications to be developed with trustless architecture. We’re not compiling an exhaustive list of real-world use cases. Instead, the following section introduces how use cases result in functional requirements for digital Identity..

See the following table with three columns which states the name of the use case, a brief description as well as a column on the functional implications for a digital Identity on the blockchain. Other implications are not covered. (eg. cash(tokens/escrow) on ledger for RTGS).

|  |  |  |
| --- | --- | --- |
| **RTGS** | Real time gross settlement, exchanging assets in real time using DvP (delivery versus payment)- as opposed to netting | *Lifecycle of Identity, delegation, revocation* |
| **Permissions / Access Management** | Roles can be assigned to specific identities, so authorities can efficiently manage permissions across their networks. For example, an employee’s unique ID might be added to the list of research technicians allowed to enter a controlled lab environment. (this is an access control list solution. Alternatively the technician can be given a Object Capability to access the lab) | *On-boarding, revocation* |
| **Education** | With a DLT for various credentials, recruitment and hiring are much simpler. Verification of claimed achievements mitigates risk of potential employees misrepresenting their skills. | *Verifiable Credentials* |
| **Supply Chain** | Not only people have identities! Physical assets can be tracked using a DLT which stores continuous data, e.g. temperature. This could streamline the arbitration process, if there is ever a shipment of rotten produce or spoiled meat. | *Identity of IoT* |
| **Identifier Autonomy** | What does owning your personal data mean to you?  *“Hyperledger Indy provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo.”* | *[self-sovereignty / privacy]* |
| **Health Records** | **(volunteers- Bill, Ankit, Robert Miller, Brian Ahier)** ((should you reach out to Adrian Gropper)) |  |

# Standards & Regulations

1. Regulations: eIDAS, PSD II, GDPR, MiFID, MAS, Aadhaar
2. Standards: OAuth, UMA, OpenID, SAML, FIDO, LDAP
3. Emerging Standards: DID, DID Auth, JSON-LD, XDI, JLINC, Verifiable Credentials, Verifiable Credentials Exchange

Sometimes, it is difficult to see where regulations stop and standards start.

## European Schemes

In contrast to schemes that develop outside sovereign boundaries like the IETF or W3C, many EU schemes have developed through trans-national legislation where the structure of the EU in terms of the legislative and consultative apparatus comes to bear. These schemes are globally important due to the fact that the commercial scale and adoption by large enterprises will foster these practices in other jurisdictions due to the virtuous cycle and technical solutions being adopted globally. As far as Blockchains are concerned, and Hyperledger in particular, these identity schemes have to be adhered to; specifically in terms of data localization as well as the right to be forgotten.

### eIDAS

The 2014 eIDAS regulation which primarily applies to PtoC (Public to Citizen) services, is a comprehensive electronic identity framework in the EU. This includes an EU-wide mutual recognition framework for eID schemes notified by member States to the EU Commission, which comes into effect on September 28, 2018. To take just one example, a Finnish student will be able to use their Finnish eID to enrol in a Spanish University. The eIDAS regulation includes a detailed description of the required attributes for eIDs as well as a LoA (Level of Assurance) framework structured around three tiers – Low, Substantial and High. This means that, when a service provider requires a minimum Substantial LoA level for its services, it will have to accept all Substantial and High eIDAS-notified schemes without discrimination and irrespective of the notifying Member State. The integrity of the framework is reinforced by the fact that the notification of an eID scheme by a member State makes it fully liable if the scheme is proven not to meet the relevant LoA framework.

A number of EU governments are now in the process of notifying eID schemes, which means that the eIDAS framework is inherently ‘Sovereign’. This means that a major hurdle towards eIDAS notification is the member State accreditation.

However, whilst the eIDAS framework is designed for Public-to-Citizen services, not the bulk of private sector uses, there is a clear recognition that the take-up of eIDs can be greatly accelerated if the private sector, and especially the banking sector, is actively involved.

In terms of Blockchain Identity, since the eIDAS scheme is approved EU wide, even if the implementation may not use Blockchains, any serious implementation of Blockchains in the EU that is in the public realm needs a bridge to this scheme which is legal and regulated; this can be considered a legacy system supported by the Enterprises that are in the Blockchain consortium. As as you can see later, under the eID scheme which has a private angle and designed to build a GDPR compliant solution, which may be implemented using Blockchains, especially using an Self-Sovereign Identity (SSI) model.

Relationship to *The Domains of Identity*: eIDAS is focused on two domains and Government Registration (getting an eIDAS) and then being able to use it with Europe Governments other than the one that issued it - thus the Government Transaction Domain and maybe also a secondary government registration with the second government.

### PSD2

With entry into force on January 12, 2016, the Revised Directive on Payment Services (PSD2[[1]](#footnote-0), Directive *(EU) 2015/2366*) aims to improve the eCommerce industry through an efficient and effective framework that creates a cross-border environment. This is an environment on payment services in the internal European Union (EU) market. It repeals the prior Payment Service Directive (PSD[[2]](#footnote-1), *Directive 2007/64/EC*) and amends other directives[[3]](#footnote-2).

The need to update the PSD was submitted on 2013. On October 8, 2015, the European Parliament adopted the European Commission proposal to create a safer and more innovative European payment system. Since its entry into force, EU member states have had two years to prepare their national regulations to incorporate the changes presented. Finally, the rules of this directive have begun to be applied with date of January 13, 2018.

Since the need for a European payment services’ regulation was materialized on 2007, the consumer point-of-view (security and user experience) was in scope regarding online payments, trying to regulate payment services and Payment Service Providers (PSP). While the changes were focused on banks, the FinTech and other technology companies remain outside the original framework of the PSD. The intention was to increase European banks and FinTech companies’ competitiveness, while creating a fair environment balancing the consumer protection and the provider obligations. The PSD2 targets consider consumer identity protection as its challenge:

* Create an environment in which electronic transactions are duly signed and protected with the use of certificates
* Mitigate fraud by authenticating transactions
* Normalize new payment methods (ePayments)
* Create a single market for payments in the EU
* Match the opportunities in the market between member states
* Match the opportunities in the market between payment services

These new rules force the providers to expose API’s that allow Third-Party Providers (TPP) to access its infrastructure in a secure manner. They will be able to gather and store information such as banking accounts and make payments, filling the transaction information and informing to the initiatory commerce. Always will be mandatory to ask the customer for authorization, and these services will always be authenticated.

Services opened for TPP’s and PSP’s will collect two main operations:

* Services that collect and store the information of the different customer bank accounts in one place
* Services to make online payments (initiation of payment services)

When the banks finally adopt the PSD2, the online commerce communication flow will be simplified from the commerce to the account, via their new API, removing intermediaries form the equation, like electronic payment providers and the interbank network (Visa or MasterCard). The consumer will be the one authorizing the commerce to execute the payment in his/her name through his/her banking account.

Initially, banking had to accomplish this work by September 2018, but the European Banking Authority (EBA[[4]](#footnote-3)) was making changes on its Regulatory Technical Standards (RTS) and guidelines, which define how the PSD2 is to be implemented. That delay supposed an attached delay on the time cap which has been postponed one year. The changes made around payments and electronic money will finally ensure that payments across the EU are secure, easy and efficient.

EBA also regulates the Interchange Fee Regulation (IFR), the security of internet payments (through its ‘EBA Guidelines’), and financial innovations in the payments sector, such as ‘virtual currencies’.

Relationship to *The Domains of Identity*: It is focused on requirements related to Commercial Transactions.

### MiFID

The Markets in Financial Instruments Directive 2004/39/EC (MiFID) establishes the general framework for a regulatory regime for financial markets. A vast set of new European Union rules known as MiFID II enforced unprecedented transparency for financial service providers (banks, asset managers and advisers) which went into effect January 2018. According to article 25(2), from the market transparency and integrity section, then defines that: “Member States shall require investment firms to keep at the disposal of competent authority, for at least five years, the relevant data relating to all transactions in financial instruments which they have carried out, whether on own account or on behalf of a client, also: “records shall contain all the information and details of the identity of the client, and the information required“.[[5]](#footnote-4)

Investment firms must report transactions in any MiFID II financial instruments to their local regulator or approved reporting mechanism no later than the close of the following working day. Under MiFID II, each individual transaction report can contain up to 65 fields, including:

* specific details of participants, including the Legal Entity Identifier (LEI code) o counterparties, funds and individual accounts
* significant additional personal details (National ID) of the natural persons.[[6]](#footnote-5)

Traditionally investment firms quality checks data against multiple sources, but this brings possibility of using blockchain inspired smart contracts, the reconciliation of data can happen in almost real time for all participants, anonymously.

In short, due to MiFID II the rules for investment companies have become more detailed, and the pretrade and post-trade transparency obligations have been extended to financial instruments other than listed shares. The operators of a trading venue (this involves operators of Multilateral trading facilities and Operating trading facilities, this may also be investment companies) must keep at the disposal of the competent authority, for at least five years, the relevant data relating to all orders in financial instruments which they have carried out.

### GDPR

The EU General Data Protection Regulation went into effect in May 25th, 2018. This regulation is intended to standardize personal data protection laws across the European Union and extends to anyone living within the EU. GDPR represents sweeping legislation as to how personal data is acquired, stored, marketed, etc. The aim of the GDPR is to put control of data back in the hands of the users. The GDPR does not affect only those businesses within the EU, but rather any that offer goods or services to EU residents regardless of where the enterprise may be established.

For our purposes, the focus is to point out considerations when using PII as defined under GDPR in DLT/blockchain solutions. The right to have one's data deleted and to contest automated decisions are perhaps those with the most far reaching implications and challenges to DLT/blockchain usage. Best practices in DLT/blockchain is not to incorporate PII in public ledgers. The use of PII in private ledgers would still require consents, storage methods, breach reporting, etc. in accordance with GDPR. If there were ever an application to make a private ledger public, thorough privacy research under GDPR would be required. While the GDPR and Blockchain technologies share many of the same guiding philosophies such as giving control back to users, mistrust of centralised systems, etc. they also clash on many fronts. Concerns have arisen about the accountability requirements of the GDPR clashing with the governance of DLT, the ramifications of storage limitations and the right to be forgotten for immutability, data transfers to foreign countries within the network that lack of sufficient safeguards, etc. In summary; keep PII out of DLT/Blockchains or at least restricted to a prunable or encrypted script, further be aware of data localization rules and ensure that data, even proofs are localized if possible. There are grounds for legitimate use and retention that could broaden the scope a little.

Relationship to *The Domains of Identity*: GDPR is focused on supporting individuals controlling their own personal data in **Civil Society Transactions** and **Commercial Transactions** and being able to move the data generated in those domains into a personal cloud in the **My and My Identity** Domain.

## 

## Other Sovereign States

### Aadhaar

Aadhaar is the largest Biometric Identity Database in the world providing identity to 1.2 Billion residents of India, which is verifiable online using their biometric.

The Aadhaar identity is in the form of a unique 12 digit random number assigned to each resident, post a deduplication process which involves biometric and demographic data collected during enrollment process. This number is devoid of any intelligence and does not profile people based on caste, religion, income, health and geography.

Aadhaar Identity is being leveraged to

1. *Uniquely identify beneficiary*, which enable entities to clean up the data. Government service delivery has been big beneficiary by seeding Aadhaar in their database. Seeding helped them eliminate duplicates and fakes, thus saving significant amount in leakages and solving the problem of inclusions and exclusions.
2. *Verifying identity of the beneficiary online at the time of service delivery*, which has brought in significant improvement in the processes. Two APIs are available to entities (both Public and Private sector) to verify the claim of the person (Authentication) and provide basic Know Your Customer (KYC) details of the person post authentication (e-KYC). The APIs work on 1:1 match with Aadhaar and Biometric and/or OTP as input.

These APIs on this database has transformed the public delivery system and ensured transparency and targeted delivery of benefits. The APIs are also utilized by the Private sector for instant delivery of services like getting a phone connection or opening a bank account. This has also enabled doorstep banking in the rural areas, which were largely unbanked.

Aadhaar identity platform with its inherent features of Uniqueness, online Authentication, and e-KYC, has enabled the Government of India and Private sector to ensure delivery of various subsidies, benefits and services to all its residents.

(Ref: www.uidai.gov.in)

Regulations and Data Privacy in Aadhaar

THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016 (Aadhaar Act) was notified by Government of India on 26th March, 2016.

(Ref: [https://uidai.gov.in/images/the\_aadhaar\_act\_2016.pdf)](https://uidai.gov.in/images/the_aadhaar_act_2016.pdf)

The Aadhaar Act defines the role of UIDAI as an authority and limits the role of UIDAI as an Authority to provide Identity to the Residents of India, primarily for the purpose of Targeted Delivery of Financial and other Services provided by the Government.

Also, Chapter VI, Protection of Information, covers the laws around protection of Information of the Citizens collected by the Authority. This Chapter has clearly put down boundaries of the information sharing.

Further regulations published on 12th September 2016, clearly defines roles and responsibilities of the Authority, and all the stakeholders in providing Services around Identity Ecosystem. The regulations have specifically taken care of aspects of Data Privacy and importance of Citizen Consent before any Authentication request and Data sharing. Any activity or retention of data in the ecosystem is bounded by consent of the Aadhaar holder.

(Ref: [https://www.uidai.gov.in/images/resource/Compendium\_June18\_03072018.pdf)](https://www.uidai.gov.in/images/resource/Compendium_June18_03072018.pdf)

The discussions around surveillance by the Government or other conspiracy theories are misplaced. The law provided clear boundaries to the Authority managing the identities.

India is having its challenges to ensure social benefits reach the last man. Aadhaar has been successful in addressing the same.

Blockchain and Aadhaar

There are two primary concerns that is being raised for Aadhaar; Data Security and Privacy. The the debate including the arguments in the courts have been centered around these topics.

Data Security

The main concerns with the Aadhaar database is being raised is that it is a centralized database and any breach in the security makes the data vulnerable. Accessibility of the data is not open to the internet thus possibility of that happening is minuscule.

There are entities who are designated as Aadhaar User Agencies (AUAs) can access the APIs for authentication and eKYC post biometric or OTP match. They do not have any access to query the data.

Data Privacy

Another concern that has been raised is the data privacy as the data can be shared with entities without the consent or knowledge of the Residents (Data Owner). There were reports where data has be leaked from the AUAs (<https://www.financialexpress.com/india-news/after-jharkhand-personal-aadhaar-details-now-leaked-on-pds-website-shocked-authorities-order-probe/641904/>). In such cases AUAs have the responsibility to protect the resident data once they receive it from UIDAI.

For both the above concerns Blockchain can provide a solution without affecting the implementation of Aadhaar. The Aadhaar eKYC can be restricted to authentication and eKYC by Blockchain wallets, which would create a Decentralized Identity based on Aadhaar biometric authentication. This identity would have trust of Aadhaar eKYC (which is digitally signed). Any further transactions will be done on this identity by the resident. The resident can create multiple identities for different domains to transact with trust being provided on the basis on generation of this identity.

Further it would be resident’s prerogative to share what kind of data with entity thus no data can be shared without consent by the data owner.

All the transaction will be logged in a Blockchain Ledger. Resident will have control over the data and the transactions and will have access to all the identity transactions.

### MAS

Monetary Authority of Singapore (MAS) is the central bank of Singapore and also acts as the financial regulatory authority, MAS is promoting a strong corporate governance framework and close adherence to international accounting standards. MAS is also a leader on financial technologies, rolling out number of initiatives related to Blockchain, encouraging FIntechs.

MAS issued guidelines to financial institutions on the use of technology to improve non face to face client on boarding, as a result MyInfo was rolled out in 2016 allowing customer to open an account without providing documentation.

Individual logs in MyInfo with 2FA SingPass, verifies and enrich personal data and gives consent to the retrieval of data. Verification of data is done by 7 public agencies.

User can use MyInfo to validate online transactions, an also be alerted when an e-service uses personal data. E-services can rely on an [API](https://myinfo-api.app.gov.sg/dev/specs/2_0) to use it. MyInfo is centralized, managed by the government. In 2017 MAS authorized a KYC Blockchain prototype where the identity data is decentralized.

## OAuth

An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications. Initially proposed in 2006, this has been updated to OAuth 2.0 [[RFC6749]](https://docs.kantarainitiative.org/uma/rec-uma-core.html#RFC6749). OAuth deals only with authorization, it has to be twinned with methods of authentication to create a full fledged solution. OAuth is an authorization protocol. As part of authentication SAML response an access token is shared with applications (mobile/web) seeking access on behalf of the user.

Request Flow:

User requests access to application > Service Provider (Application) redirects request to Identity provider (IDP) > idp presents login page > User enter id/password > IDP authenticates user and sends a signed SAML reponse to SP > SP allows user to browse the protected resource

(OAuth only) The response includes an access token which the application can use to gain direct access to the identity provider's services on the user's behalf.

### UMA

User-Managed Access (UMA) is a profile of OAuth 2.0 . UMA defines how resource owners can control protected-resource access by clients operated by arbitrary requesting parties.

## VRM

VRM stands for Vendor Relationship Management. It is the obverse of CRM which is Customer Relationship Management. Vendors seek to capture their customers and keep the relationship sticky. This is often based on the data that they gather and hold on to. VRM seeks to put the customer at the center and works on developing solutions that allows customers to switch between vendors

## OpenID

OpenID is an open standard and decentralized authentication protocol. It allows users to be authenticated by co-operating sites (known as relying parties, or RP) using a third-party service eliminating the need for service provider/application owners to provide sso or auth systems and enabling users to login with one set of credentials on different websites.

## OASIS

## OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

## SAML

SAML Security Assertion Markup Language is an OASIS standard to pass user identity attributes as required by the identity provider (SSO) in order to authenticate a user into an application/system.

### Request Flow:

User requests access to application > Service Provider (SP) (Application) redirects request to Identity provider (IDP) > idp presents login page > User enters id/password > IDP authenticates user and sends a signed SAML response to SP > SP allows user to browse the protected resource

## FIDO

## LDAP

LDAP - Lightweight Directory Access Protocol is based on subset of X.500 standards. X.500 is a series of computer networking standards covering electronic directory services.

LDAP enables clients to search, retrieve, store data such as username and passwords; allow applications to authenticate/validate users

# Identity Warriors

## Verifiable Claims Working Group

The Verifiable Claims Working Group at the W3C is developing standards for expressing and exchanging "[claims](https://www.w3.org/TR/verifiable-claims-use-cases/#dfn-claim)" that have been verified by a third party and to make them easier and more secure on the Web. The emphasis on making these claims transportable to ease ownership and control of user credentials.

References :

https://www.w3.org/2017/vc/WG/

https://www.w3.org/TR/verifiable-claims-use-cases

## RWOT

Rebooting Web of Trust has been an unconference style design workshop with the focus of taking ideas that have been cultivated within the identity community and create complete white papers (and in some cases early specifications or code) that can be published and disseminated to a broader group of stakeholders who rely upon the work in the identity community. Typically there are two events per year. The primary focus of the events is to produce first drafts of 5-7 papers that can be turned into final drafts in between events. Of the papers that have been widely cited from the first RWOT event is the [DPKI (Decentralized Public Key Infrastructure)](https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/dpki.pdf). More recently, one of the main papers that has emerged from this event is the [Decentralized Iidentifiers (DID) spec](https://w3c-ccg.github.io/did-spec/), which is now through the standardization process at the W3C Credentials Community Group.

## ID2020

From the early inception of the ID2020 ALLIANCE (circa. 2017), the *vision* (and subsequent goal) of its founding member groups and stakeholders has been “*how individuals could be empowered with a* ***secure, portable digital identity*** *and a respected voice in the nascent conversation about digital identity in humanitarian contexts*…”.

Today, the ID2020 Alliance has assembled a group of key, committed partners to *move from vision to implementation*, comprising an growing membership of organizations and knowledge-based forums & workshops involving the WEF, UN\_UNHCR (for refugees & other groups), OCHA, UNDP, The Rockefeller Foundation, Accenture, Microsoft, IBM and associated third parties.

Global environmental and geo-political pressures combined with growing political willpower, provide a mandate for the ID2020 Alliance to make “*a coordinated, concerted push towards the goal of* ***universal digital identity***”, adhering to best-practice standards to enable personal, persistent, private and portable identities.

Reference ID2020 site, via *https://id2020.org*

## IIW

## DIF

The [Decentralized Identity Foundation](http://identity.foundation/) is an open-source consortium of developers and companies working together to build standards and implementations for foundational building blocks for identity solutions. They are focused on [working code](https://github.com/decentralized-identity) over being a “talking shop” or on getting to ultimate solutions.

DECENTRALIZED IDENTITIES anchored by Blockchain IDs linked to zero-trust datastores

that are universally discoverable.

As of May 2018 there are [56 member companies](https://medium.com/decentralized-identity/decentralized-identity-foundation-grows-to-56-members-in-our-first-year-3ec117e811d8). Hyperledger is a member of the DIF consortium. DIF is an associate member of Hyperledger. Many Hyperledger member companies are also individual members of DIF. Pretty much every company working on identity solutions is a member of the DIF, spanning all blockchain base tech stacks.

## Sovrin Foundation

Established in September 2016, the Sovrin Foundation is an international non-profit foundation created to govern a global public utility for decentralized identity. The Sovrin Foundation adds a legal framework on top of the technical foundation provided by Hyperledger Indy.

The Sovrin Trust Framework is the legal foundation of the Sovrin Network as a global public utility for self-sovereign identity. The Sovrin Trust Framework governs how trusted institutions, called stewards, will operate validator nodes of the Sovrin Network. All stewards will run an instance of Hyperledger Indy.

The Sovrin Network is only one network designed to run Indy; any number of other networks may be created to run their own instances.

# Implementing Identity Schemes

tools for building actual systems  
Each needs a volunteer- except for ones noted explicitly

## Public Key Infrastructure (PKI)

Digital Identity was not supported in a foundational way in the basic Internet protocols, including http. As digital commerce and other commercial interactions became prevalent, it became necessary to establish the Identity of the parties and also allows secure communications. Public Key Infrastructure (PKI) refers to the infrastructure which supports Public Key cryptography also known as asymmetric cryptography. This infrastructure is responsible for securing electronic interactions on the web today. PKI binds the public keys of entities to their identities, who possess a secret(a private key) that corresponds to their public key. Verification of certificates is done by a Registration Authority (RA). These verifications are in digital certificates signed by a Certificate Authority (CA), which can be verified by using the CAs public key. A Validation Authority (VA) checks the credentials before establishing a secure session, a list of well known CAs are included in popular browsers. Breaches of CAs, timely revocation, lack of recourse in case of false representation (breach of RA) have raised questions; proposed solutions include auditing of CAs as well as Distributed PKI (DPKI).

Normally individuals do not obtain a public digital certificate; these are obtained by organisations and entities that seek to establish that they are who they say they are. Entities like banks, e-commerce firms, news sources and others who need to firmly establish the identity controlling a website before people trust to engage in digital interactions.

The other model followed is self-certification and the building up of a web of trust, since anyone who relies on a certificate issued by a CA ultimately relies on the security of the CA itself.

## Central authority – Federated authority-

Describe CAs

## X.500 & LDAP Systems-

Defined under the X.500 PKI Standard maintained by the International Telecommunications Union (ITU), this standard was developed as a joint activity between the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The most recent ITU Recommendation for X.500 –a recommendation being a commercial analogue to the Internet’s Request for Comment (RFC) mechanism- is dated 2016-10-14. X.500 is defined using the Open Systems Interconnect (OSI) model but because most use of PKI takes place in a world dominated by TCP/IP, its comprehensive scope is not purely implemented in practice.

The most commonly used directory implementation derived from X.500 is the Lightweight Directory Access Protocol (LDAP). Originally developed at the University of Michigan, it has grown from a simpler means of implementing the directory to a much more comprehensive standard itself. LDAP supports the creation and maintenance of a directory of *identities*.

An *identity* is associated with multiple sets of data, the most basic of sets comprised of a parameter and its value. Typically, these sets refer to an object and permissions granted to the identity for that object (e.g., read customer table, create user) .

LDAP’s primary functions comprise add identity, modify identity, delete identity, and search for identity. To ensure the integrity of the directory, there are additional functions (e.g., Bind, Unbind) required to establish a trusted connection with an LDAP server.

*[Need to address the supported operations in the context of the PKI section, above]*

The most common form of PKI certificate employed is X.509. [TO BE CONTINUED]

X.500 References

1. [ITU X.500 Recommendation](https://www.itu.int/rec/T-REC-X.500-201610-I) (behind paywall). Last accessed 2018-03-19
2. [X.500 or LDAP](http://faculty.wwu.edu/auer/MIS423/X.500/Directories%20and%20X-500%20-%20An%20Introduction.pdf) Last accessed 2018-03-21

## Self-Sovereignty

Concept

## DIDs & Verifiable Claims

Describe current standards

## Interoperability

How would DiD->DiD Document->verifiable claim interact with Legacy, Blockchains with Legacy- How would chains interact-DiD TLS

**Canonical forms of Identity**

**Self Sovereign Identity**  
Self-sovereign identity also called self-managed identity or user-controlled identity is a lifetime portable digital identity for any person, organization, or thing that does not depend on any centralized authority and can never be taken away.  
<todo add more detail>  
   
**Decentralized Identifiers** (DIDs) are very useful for SSI, but there are also other types of identifiers that could be considered "self-sovereign", e.g. local names (petnames) or cryptographic identifiers (cryptonyms, CIDs). DIDs are a type of globally resolvable, cryptographically-verifiable identifier registered directly on a distributed ledger  
  
**Structure of DIDs** derived from URN Syntax (RFC 8141)  
  
urn:uuid:ae84-d5c2-9fb785ea-72cd34  
<Scheme>:<Namespace>:<Namespace-Specific Identifier>  
  
Mapping from URN to DID Syntax  
  
did:sov:3k9dg356wdcj5gf2k9bw8kfg7a  
  
<Scheme>:<Method>:<Method Specific Identifier>  
  
 Some examples of different methods: <todo insert table here>  
   
  
**How does DID map to DID Document**?   
  
{ “Key”: “Value” }  
  
{ “DID”: “DID Doc” }  
  
{<Decentralized Identifier>:< DID Document (JSON-LD) >  
  
**The primary elements of a DID doc**  
DID (i.e., the JSON-LD is self-describing)  
List of public keys (for the owner)  
List of service endpoints (for interaction)  
Access control branch (for key mgmt)  
Timestamps (for audit history)  
Signature (for integrity)  
   
  
The decentralized identity “stack”  
  
<picture>   
  
Verifiable claims are the new format for interoperable digital credentials being defined by the W3C Verifiable Claims Working Group  
  
W3C Verifiable Claims Ecosystem  
  
<picture>  
  
 Use of Verifiable Claims  
  
<picture>  
  
 URN

* DID->DID DOC
* X.509-X.500
* Biometric?

# Identity models

## Sawtooth:

The Endpoint Registry transaction family manages information about Sawtooth network endpoints. In theory, an endpoint can be any object with a role in the Sawtooth validation network. In practice, the registry primarily contains information about network endpoints participating in ledger validation.

An endpoint first submits a Register transaction to establish a persistent network identity. Generally, the endpoint provides basic information (a name, a ledger domain, and its public key) and enough additional information, in the form of a ValidationObject, to establish its identity. Different ledgers may implement different policies for granting permission for an endpoint to register itself. For example, the (Proof of Elapsed Time) PoET consensus module requires proof that the enclave associated with the endpoint is valid and not corrupted. For any successfully registered endpoint, the validation object also implements a policy for granting permission to validate a block of transactions. For example, the PoET validation object requires that an endpoint wait several blocks after registration before it may validate a block in the ledger.

Registration of an endpoint simply grants permission for the endpoint to participate in the validation process. An endpoint actually joins the network with a Connect transaction that provides information about the endpoint’s network connectivity. Similarly, when an endpoint leaves the network, a Disconnect transaction cleanly removes the network connection. Ledgers may implement a policy that network nodes reconnect periodically to ensure that stale connectivity information is removed from the ledger.

From endpoint registry doc: <https://drive.google.com/open?id=1gWlbsKtgApOTm1E5XJsw2J3U6AvIRxujWiG-vm6ELOM>

* + Link to Fabric MSP <https://docs.google.com/document/d/1Qg7ZEccOIsrShSHSNl4kBHOFvLYRhQ3903srJ6c_AZE/edit?usp=sharing>
  + Link to Indy
  + Link to Burrow
  + Link to Fabric Composer

## Indy:

Indy aims to provide Hyperledger projects and other distributed ledger systems with a first-class decentralized identity system. In other word, Indy is a DLT specifically built for identity and identity only. Indy supports a Public-Permissioned ledger. Contrasted with Bitcoin/Ethereum being Public-Permissionless and R3 Corda/CULedger/SecureKey as Private-Permissioned.

Indy provides the following high-level features:

### Verifiable Claims:

Indy supports user-controlled exchange of verifiable claims, with a rock-solid revocation model for cases where those claims are no longer true. Verifiable claims are a key component of Indy’s ability to serve as a universal platform for exchanging trustworthy claims about identifiers.

### Decentralized Identifiers (DIDs)

Identifiers on Indy are pairwise unique and pseudonymous by default to prevent correlation. DIDs on the ledger point to DID Descriptor Objects (DDOs), signed JSON objects that can contain public keys and service endpoints for a given identifier. DIDs are a critical component of Indy’s pairwise identifier architecture.

### Privacy First

In Indy, personal data is never written to the ledger. Rather all private data is exchanged over peer-to-peer encrypted connections between off-ledger agents. The ledger is only used for anchoring rather than publishing encrypted data.

### Zero-Knowledge Proofs (ZKP)

Indy has built-in support for zero-knowledge proofs (ZKP) to avoid unnecessary disclosure of identity attributes—privacy preserving technology that has been long pursued by IBM Research ([Idemix](https://www.zurich.ibm.com/identity_mixer/)) and Microsoft ([UProve](https://www.microsoft.com/en-us/research/project/u-prove/)), but which a public ledger for decentralized identity now makes possible at scale.

## uPort:

uPort is an interoperable identity network for a secure, private, decentralized web.

uPort's open identity network allows users to register their own identity on Ethereum independent from any centralized authority. This decentralized model of identity forms the foundation for a user-centric data network, where users own and manage their personal data in private. On uPort, users are always in control of their data and they are free to share it with whomever they choose.

uPort built on top of Ethereum and can be implemented in both public or private Ethereum networks. The uPort protocol is implemented as a set of Ethereum Smart Contracts. The uPort team also proposed the following Ethereum Improvement Proposals (EIP):

ERC1056 EIP - Lightweight Identity

ERC780 EIP - Ethereum Claims Registry

1. Other blockchains (publicly known)
2. Other Implementations and PoCs

**PLifecycle & Key management**

* Genesis or creation
* Extinction-Natural, voluntary (right to be forgotten) or forced
* Changes-provided by owner of identity, others (accumulation of attestations)
* Key Management - lost keys and revocation, key recovery

**Interoperability of Identity**

* Bootstrapping
* Sharing: between blockchains (public vs. federated vs legacy)

**Threat surface & Threat models (limits & techniques)**

**Generic Identity Interface**

* detailed interface definition

**Proposal & project plan for an implementation**

Dimensions of Identity

* central authority or federated authorities vs Self-sovereignty
* Identity of the Infrastructure vs Identity of Transactors
* Identity of nodes vs Identity of natural persons vs identity of corporate and other entities
* Trusted Execution Environments (TEEs) and provability
* Anonymity and Privacy including unlinkability.
* Portability, Recoverability, Reissuance, Revocability [Sanjay@Intel]
* Claim Composability between public and enterprise [Sanjay@Intel]
* Reputation, Personas, Delegation to proxies [Sanjay@Intel]
* Biometrics [Danny@IBM]

**Contributors**

Christopher Allen

Kaliya Young

William Sparks

Nitin Agarwal

Vipin Bharathan

Sze Wong

Eric Bourdin

**References**

1. [A primer on Functional Identity](https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/functional-identity-primer.md), Joe Andrieu 2017 last retrieved May 2nd, 2018
2. Young, Kaliya. Domains of Identity. Identity Woman, 2018, www.identitywoman.net/domains-of-identity
3. Identity WG Meeting notes:<https://docs.google.com/document/d/1nVkjhSlghjc4KFWEYDU2B0ztWCFh1CK8a7VmqwFsnKY/edit?usp=drivesdk>
4. [Projects/companies working on blockchain and identity](https://github.com/peacekeeper/blockchain-identity), managed by Markus Sabadello last retrieved May 2nd, 2018.
5. [Laws of Identity](https://msdn.microsoft.com/en-us/library/ms996456.aspx) Kit Cameron 2005 last retrieved May 2nd, 2018
6. Verifiable Claims, https://www.w3.org/TR/verifiable-claims-use-cases/
7. STL end-point registry:<https://drive.google.com/open?id=1gWlbsKtgApOTm1E5XJsw2J3U6AvIRxujWiG-vm6ELOM>
8. Fabric MSP

<https://docs.google.com/document/d/1Qg7ZEccOIsrShSHSNl4kBHOFvLYRhQ3903srJ6c_AZE/edit?usp=sharing>

1. Indy-Sovrin

https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

<https://www.hyperledger.org/blog/2017/05/02/hyperledger-welcomes-project-indy>

1. Burrow
2. Iroha
3. uPort

<https://medium.com/uport/the-basics-of-decentralized-identity-d1ff01f15df1>

<https://developer.uport.me/overview>

1. MAS :

KYC Blockchain Prototype

[MyInfo](https://www.singpass.gov.sg/myinfo/intro)

1. GDPR doc: <https://docs.google.com/document/d/1t1UUsoxLrmFhHgiXWPUCTlW4XFqsa8p0gy6JhpISP6A/edit?ts=59d4e1a3#heading=h.flgge0ag1yuw>   
   GDPR Article 29 working group papers

GDPR input 2 (bill):

<https://docs.google.com/document/d/1IC7BSv78EO1-SSVDQmw5rnH0uybGNUXU5RPO5AIPYfU/edit?usp=sharing>

PKI References

1. [Public Key Infrastructure.](https://en.wikipedia.org/wiki/Public_key_infrastructure) Wikipedia. Retrieved 3/15/2018
2. ["Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce"](http://apps.americanbar.org/dch/thedl.cfm?filename=/ST230002/otherlinks_files/dsg.pdf) (PDF). American Bar Association. Retrieved 3/15/2018
3. Auditing <https://www.certificate-transparency.org/>
4. <https://tools.ietf.org/html/rfc6962>
5. CONIKS <http://www.jbonneau.com/doc/MBBFF15-coniks.pdf>
6. CONIKS implementation <https://github.com/google/keytransparency>
7. POMCOR <https://pomcor.com/category/identity-proofing/>
8. DPKI <https://danubetech.com/download/dpki.pdf> Retrieved 3/20/2018
9. WebTrust - CA auditing http://www.webtrust.org

1. Legislative Framework PSD 2 (Directive *(EU) 2015/2366*): https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366\_en [↑](#footnote-ref-0)
2. Legislative Framework PSD 1 (Directive *2007/64/EC*): https://ec.europa.eu/info/law/payment-services-psd-1-directive-2007-64-ec\_en [↑](#footnote-ref-1)
3. *2002/65/EC,* PSD updates *2009/110/EC* and *2013/36/EU*, andRegulation *(EU) No 1093/2010* [↑](#footnote-ref-2)
4. Regulatory Technical Standards on strong customer authentication and secure communication: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money [↑](#footnote-ref-3)
5. Markets in Financial Instruments (MiFID II) - Directive 2014/65/EU https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu\_en [↑](#footnote-ref-4)
6. Danny Busch (2016) MiFID II: regulating high frequency trading, other forms of algorithmic trading and direct electronic market access, Law and Financial Markets Review, 10:2, 72-82, DOI: 10.1080/17521440.2016.1200333 [↑](#footnote-ref-5)