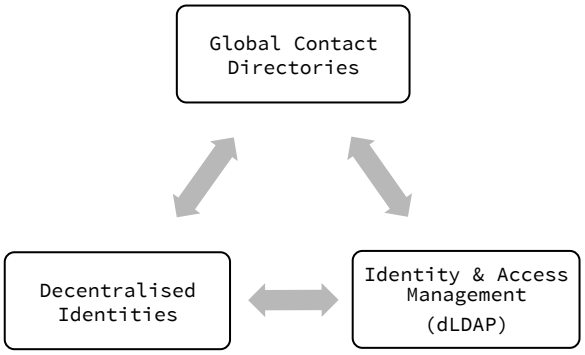
Decentralized Identity & Access Management (dIAM)

Vishal Gupta
Vinay Gupta
Nikhil Rai
Kunal Bajaj
Arjun Singh

Technical whitepaper (internal) – 1st March 2018



Decentralized IAM infrastructure and LDAP using MSISDNs with SPKI

Table of Contents

Glossary

Contact Directories – Multiple directories on a smartphone wherein each directory contains shared list of contacts across multiple devices.

dIAM – Decentralized Identity and Access Management goal is to ensure that no single third-party can compromise the integrity and security of the system as whole.

DID - Decentralized Identifiers (DIDs) are a new type of identifier intended for verifiable digital identity that is "self-sovereign" requiring a decentralized public key infrastructure (DPKI).

dLDAP – Decentralized Lightweight Directory Access Protocol is proposed LDAP service based on distributed database of MSISDNs and crowd consensus based contact directories.

DPKI – Decentralized Public Key Infrastructure that is able to preserve the integrity of identifiers by protecting organizations or individuals from private key loss or compromise.

GUID – Globally Unique Identifier used for addressing any object in digital space.

IAM – Identity and Access Management is, in computer security, the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons."

Identity Hub – A secure and encrypted data store containing information related to an identity. The data store is uniquely addressable using a DID and syncs with other hubs.

LDAP - Lightweight Directory Access Protocol is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories. The LDAP directory service is based on a client-server model.

MFA – Multi-factor authentication is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism.

MSISDN – Mobile Station International Subscriber Directory Number is a number used to identify a mobile phone number internationally. MSISDN is defined by the E.164 numbering plan.

OIDC – OpenID Connect is an authentication layer on top of OAuth 2.0, an authorization framework. The standard is controlled by the OpenID Foundation.

PGP – Pretty good Privacy - an early public key application, defining the first public key infrastructure to be widely deployed.

PKI – Public Key Infrastructure is used to digitally sign documents transactions, and software to prove the source as well as the integrity of those materials.

Proof-of-life – proof of existence of the real person behind the digital identity through confirmation from other socially associated mobile devices based on live human interaction as strong authentication.

SPKI – Simple Public Key Infrastructure

1. Introduction

Today's digital world lacks a credible identity system that is universally consumable and can be trusted by counter parties across industries. Further, all crowd sourcing based solutions lack credibility and verification that is needed to address regulatory requirements. Getting, all the industries, governments and consumers across hundreds of jurisdictions to agree on a framework is a challenge. A great deal has already been written on challenges in creating universal identity (Vinay Gupta, 2017). The problem has been part technical and part political.

Owning identity itself is hard for individuals

Verifying real identities requires mass consensus and adoption

Centralized systems are unreliable in long term due security and political risks

Identities need to constantly remain validated and updated

Limitations of mass adoption by different stakeholders

As we rapidly adopt digital technologies with smartphone penetration slated to reach 4 billion by 2022 and new technologies like IOT, blockchain, AR/VR and digital currencies getting ready for mainstream adoption, the need for cybersecurity has never been greater.

The identity theft losses are reaching $16b[1] annually in USA alone. The cost of KYC & AML is $15bn in the financial industry only. The latest forecast from Gartner Inc. says worldwide information security (a subset of the broader cybersecurity market) spending will grow 7 percent to reach $86.4 billion (USD) in 2017 and will climb to $93 billion in 2018. Global spending on cybersecurity will exceed $1 trillion cumulatively over the next five years, according to Cybersecurity Ventures.[2] [Cybercrime attacks are expected to cost us $6 trillion a year by 2021. In a single year, cyber terrorism could cost us three times more than the entire U.S. housing and real estate industry is currently worth.

The Chairman of IBM calls it the "greatest threat to every profession, every industry, every company in the world". Cisco cites a report saying it will be more profitable than the global trade of all major illegal drugs combined. ATT calls it the greatest transfer of economic wealth in history.][3]

The identity data today, lies fragmented and owned by different corporations, having conflicting monetization objectives. It's often secured by fragile passwords or rely on one-time passwords for recovery that are easy to hack with commonly available tools. With the explosion of web content and services, it has become hard to keep track of logins, profiles and passwords. MSISDN based one-time passwords still offer a temporary relief but the system is extremely vulnerable to hacking, lacks identity attributes and has no identity verification.

On the other hand, social networks are limited by the number of people who join, remain centralized and committed to conflicting incentives to monetizing the identity data they are trusted with. They often subject the users to undesirable social noise and comparison. This positions them at odds with consumers volunteering data to build strong profiles. Further, the social footprint created on such networks still rely on the users to update the social profile without any real external validations. This has enabled the prevalence and spread of fake identities.

Government and Industry are desperately looking for a solution.

"More than 100 developing countries lack functional civil registration and vital statistics. Some countries like Malawi and Ethiopia have registration rates in the single digits. Experts estimate that there are 1.5 billion people without a legal identity. That's the equivalent of all of China going untracked.

[1] https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html
[2] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[3] https://www.prnewswire.com/news-releases/caught-napping-on-bitcoin-cyber-crime-solutions-are-next-655554243.html

Providing everyone on the planet with a legal identity would expand access to democracy, unlock economic and legal rights, facilitate the provision of healthcare and education, and accelerate global economic development. In fact, it's hard to overstate the implications if we were to get this right." (ID2020.org, 2016)

Gartner believes a decentralized identity model that is built on a common identity trust fabric will become more feasible in the coming years. (Gartner, 2016)

Governments are now holding businesses and banks responsible for AML and KYC. Europe has recently witnessed a complete overhaul of data privacy under GDPR that is going live in May 2018 putting steep penalties on breaches. All countries are likely to follow suite.

2. Understanding the technical challenges

2.1 Owning Identity is hard

An average consumer is not technologically inclined. Besides having technological and cryptographic challenges, owning identity without proper safety and recovery is dangerous. Permanent loss of control or hacking can lead to severe consequences. Owning an identity today is a technological challenge for an individual as it requires:[Comment: Are the below supposed to be desired features?]

- **Associating public keys with Identity** – a public ledger is needed for identity lookups and making sure each identity is uniquely represented by a person. The ledger would typically contain the public key and would be located on a public blockchain.
- **Modify and control identity attributes** – a privately owned profile or profiles containing a list of attributes and values that can be added, modified or revoked.
- **Regaining lost control of Identity** – owners need to have unrestricted access and right to regain control or reset keys in case of a compromise without the need for centralized authority.
- **Selective sharing of attributes** - a way to share signed copies of identity attributes with third parties. The third parties should be notified when such attributes become invalid or expire.
- **Collect third party claims and authorizations** – a method to collect & further share third party certificates containing claims or authorizations.

2.2 Verifying identity requires mass consensus

Digital identities have had two broad concerns.

Synthetic Identities – wherein the actual person does not exist and the identity is digitally constructed.

Identity theft – where the attacker is masquerading as someone else. The digital identity is hijacked. This person may or may not be known to the real owner.

In these cases, you need mass consensus or organizations to validate if the real person actually exists. These both can not be solved by biometrics. It's often misunderstood as a means to protect against Identity theft. Unlike a password, once a biometric is compromised, it is permanent.[4] The problem with biometrics on the internet is if you transmit the biometric id or its hash to third parties then the chances of permanent compromise remain extremely high.

2.3 Centralized systems are unreliable in long term

Global identity trust fabric needs to be a decentralized system that cannot be attacked from inside or outside. A central store for identity data exposes it to mass breaches and denial of service attacks. Any exposure to such a system would render every service in the world vulnerable. identity systems also control authentication and authorization of third party services including financial transactions and therefore attract the most hacking

[4] https://www.usatoday.com/story/cybertruth/2013/09/12/why-biometrics-dont-work/2802095/

attempts. Further, a centralized system also renders the system vulnerable to standard geo-political and governance risks. A system having such global significance cannot afford the tiniest of vulnerabilities.

2.4 Identities need to constantly remain validated and updated

Stale or incorrect information might be worse than no information. The identity data needs to be routinely validated and kept up-to-date. People loose mobiles, change numbers, IDs expire, move homes, switch jobs, or even countries, get married or just change names. This needs to be synced across with service providers, institutions, registries and government records to avoid confusion while maintaining privacy.

2.5 Limitations of mass adoption

Existing networks and databases are limited by their reach in verifying identities to their existing users. The identity trust fabric needs to function with fraction of people signing up and avoid the classic chicken and egg bottleneck.

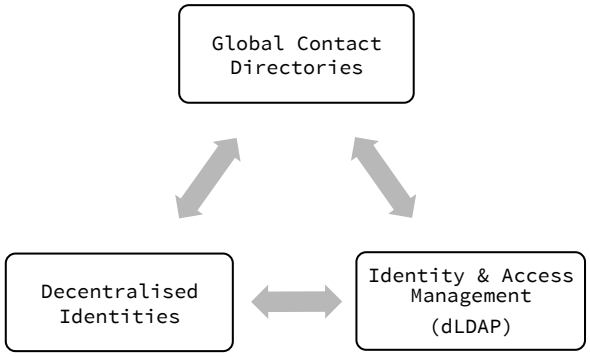
2.6 Cyber-security can no longer be a walled garden

- Tens of specialized cloud services being consumed as technology stacks
- Multi devices including smartphones are now a norm
- Remote working and work from home is more common
- Bring your own device
- Authorization information embedded along with digital assets
- Cloud collaboration is replacing Virtual networks

Many companies with 250 or fewer employees have learned the hard way that if they wait until after being hacked to deal with it — it may be too late. Nearly half of all cyber attacks are committed against small businesses, and the percentage is expected to rise next year.[5]

3. Designing - Decentralized IAM infrastructure

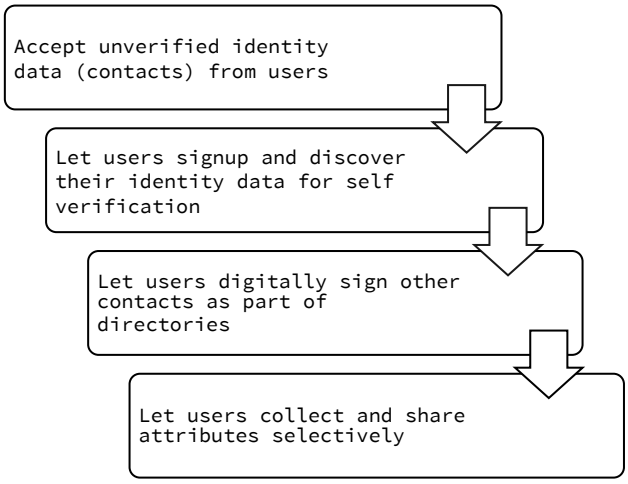
The world is rapidly shifting to cloud services and the demand for single-sign-on is rising. SMEs are consuming multiple cloud services across departments and the need for a shared directory of employees and maintaining frictionless secure access is felt even more. In this new paradigm, the authorization information now sits in respective cloud service providers while employees use multiple devices and roam freely. The complexity of network admission control and authorization information needs to be simplified mobile-first employee directories that match the working styles of today. A very useful and broad architectural layering requirements were recently proposed as Semantic Identification Layers (Reed, Architectural Layering for Decentralized Identification, 2017).



To create a dIAM – MSISDNs offer a good universal baseline to begin processing data of live identities. It can be combined with other factors like names and connections to determine unique identities. Further, existing contact lists offer a raw dump of contact information to start building graphs universally.

[5] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

The simplest way to build global identity verification is to issue certificates to identities associated with MSISDNs present in contact directories. When such MSISDNs accumulate certificates from multiple directories like company, family, resident welfare associations, schools, colleges the identity data becomes reliable. When such identities have live interaction with their loved ones, they end up validating each other as real people.



The users benefit from the organized directories on their phones. The effort of manging such directories substantially reduces for everyone directly by the number of people using it. These directories can then also be used as virtual LDAP on the cloud. The MSISDN providing a way to have password-less mobile based authentication for users. Having the user MSISDN across the directories of different organizations gives a common trust fabric that can be decentralized using a public blockchain.

4. Global Contact Directories

(Diro platform under-the-hood)

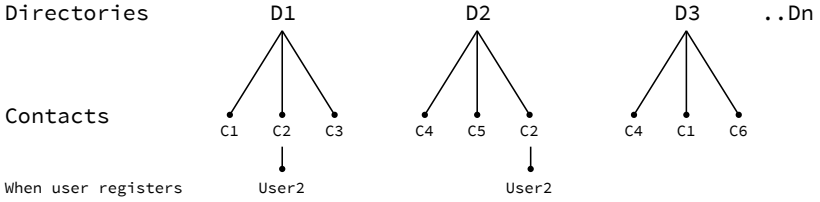
A multi-directory platform wherein users can tag their existing contacts on smartphones into one or more directories shared in closed user groups. When a user tags an existing contact into a directory then it also tags on other phones having the same directory and also containing matching contacts automatically.

4.1 Aggregate unverified identity data (contacts)

The system allows every user to upload all their existing contacts to the platform as private directories. Many caller id apps aggregate data of users to create public databases.

An average user has about 650 contacts and therefore it should be possible to get all contact data mapped within about 1% signups of the total population.

4.2 Bonding orphan contacts with owner of MSISDN



When a user registers on the platform by verifying his MSISDN, the platform automatically associates similar contacts across all the directories on the platform with his/her unique user id. It discovers the contacts in the background, using the verified

MSISDNs and other contextual factors, without impacting any privacy or ownership of the contacts in any way.

4.3 Identity attributes discovery & auto-correct

It is not necessary to make the aggregated database public and can be given to the respective owners of the MSDINs. It anonymously discovers all information matching the MSISDNs in the global database of contacts. It discovers all information related to an identity containing complete crowd data including all obsolete information to the newest data available. It helps the individual take control of the information and ability to mark all information as discarded or with most appropriate labels. (IN Patent No. PCT/IB2017/051056, 2016)

Auto-correction - then propagates the correct labels and restricts/hides the zombie data lying in all other directories and phones of other users without sharing any additional info. This is done without actually deleting any data in other directories by simply applying appropriate labels.

4.4 Creating shared directories

The directories that can be create are basically of two types.

Connected Directories (groups) – wherein the directory is shared or made accessible to all its listed members automatically whenever they sign up.

Unconnected Directories (contact lists) – wherein the directory is a private contact list only shared with specific contacts that may or may not be listed in the directory itself.

Connected Directories
Coworkers, Family, School, College Batchmates, Clubs, Projects etc.

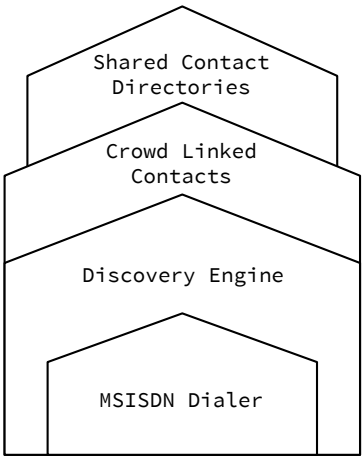
Unconnected Directories
Clients, Vendors, Friends, Consultants, Key Contacts - like Doctors, etc.

4.5 Directory discovery engine – to create shared directories

The key is to create the discovery engine that lets new users discover and automatically participate in existing directories. When a new user signs up, the system uses bonded contacts with his mobile number to search for directories that are relevant and shared with him/her. It also lets any user to create new connected or unconnected directories that may include members who have not signed up. This technology enables users to have complete directories pre-emptively and create value for users who sign up later. (USA Patent No. PCT/US2015/019443, 2014)

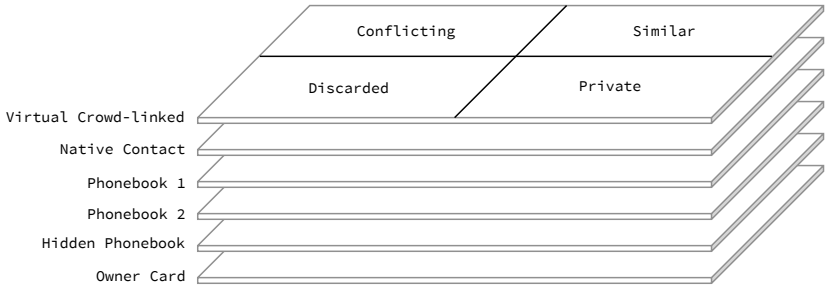
This innovation of the discovery engine is a key enabler for the crowd-mining of these directories to become possible. Forming such universally complete connected and unconnected directories is unprecedented and has many use cases across domains.

Shared Phonebooks is the most logical way forward, but it is not scalable without "Crowd Linked Contacts" & Discovery Engine.



4.6 Crowd-linked contact layers

The platform virtually combines contacts based on context on different user nodes to generate virtual contact profiles across directories. A user may have multiple contacts of a person in different directories containing with different pieces of information shared. The platform virtually combines these matching contacts for a single view to the user. The linking algorithm further calculates priority and state of different labels attached to each piece of the information while respecting privacy of the contact.

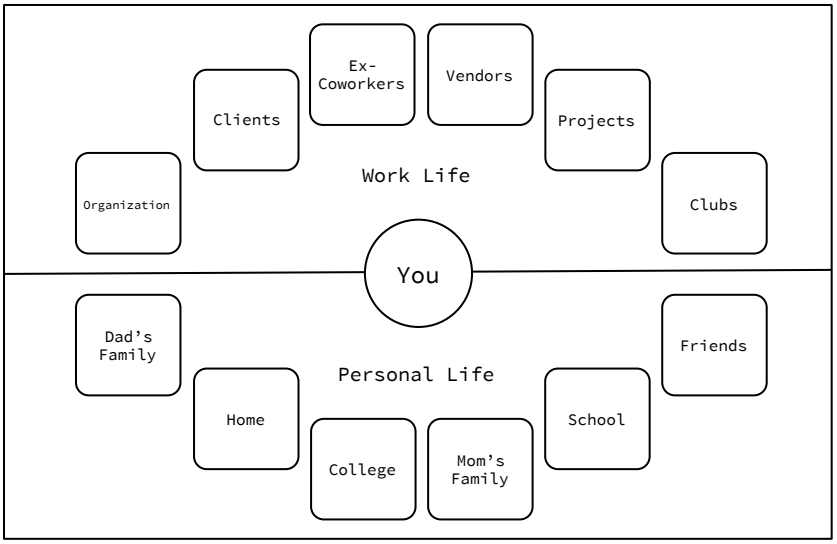


It introduces new concepts like Archive, Discard & Hide at appropriate levels to provide a hassle-free experience (IN Patent No. PCT/IB2016/055271, 2016). For example, if a user has a number for a contact discarded in one of the directories, the number would get crossed on the contact in spite of it being still active in some other directory as an override. On the other hand, if the original owner of the contact identity discards a number then it changes the label for all related contacts to that identity across the platform including the directories that are not visible to the user.

4.7 Using directories to build identity consensus

Directories act as group consensus for the identity verification. Directories based on active MSDINs (mobile numbers) are the most authentic source of identification to drive consensus across international borders. The digital identity remains dormant, private and secure on blockchain for the users to stake claim at any time.

Everyone is connected with other people based on context. Each person on an average is a member of about 9-10 connected directories. The creation of these multiple directories for each person and active phone usage with other members, creates a decentralized consensus based identity for each user, which is recorded on blockchain.



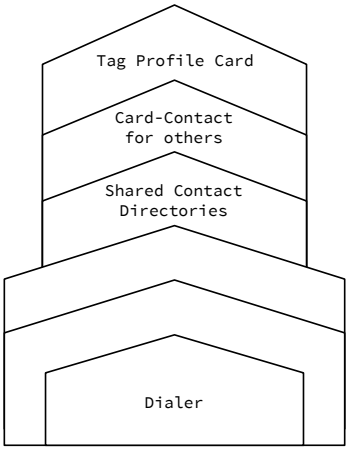
Directories enable an automatic social KYC on smartphone users. The directories themselves may be strictly controlled or built on lazy consensus. The system allows groups to validate identities automatically using digital signing in the background. For example: an employee of a large company would automatically get verified by virtue of being listed in the directory. And such multiple verifications from different official or group consensus based directories enable social KYC profiles effortlessly.

4.8 Narrowcasting engine

The identity can have multiple profile cards – that contain custom combination of profile information like Work card, Private Card, Minimal Card etc. It can then be narrow casted to each directory as additional info in two ways (IN Patent No. PCT/IB2017/053622, 2017; IN Patent No. Universal original document validation platform , 2015).

Connected Directories (groups) - User can control complete info shared in a connected directory. It does not affect any additional information other users have in other crowd linked contact layers from other directories or their own device.

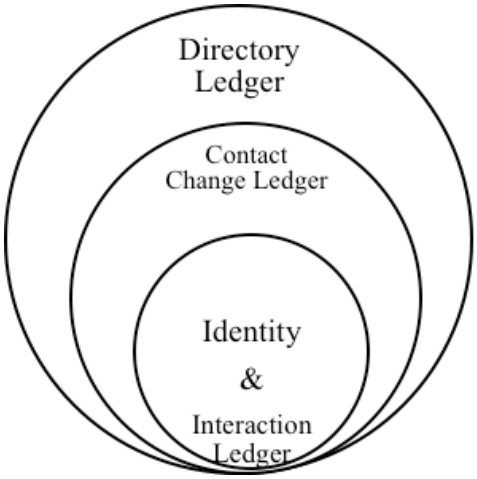
Unconnected Directories (contact lists) - User can narrow cast their information to a list of unconnected members in a directory to supplement the contact information stored in their devices in a separate layer.



Profile Cards solve privacy concerns in Crowdsourced directories.

5. Using distributed database to decentralize contact directories

For decentralizing the directories, it is important to use record chaining using hashes to manage conflicts across devices while decentralizing the control. Further lazy consensus may be used to support offline transactions.



Directory Ledger – Contains changes to members roles, permissions for block distribution with other identities.

Contact Ledger – Changes to Identity related attributes, certificates, claims, authorizations, change log etc.

Identity Ledger – Change log of MSISDN, devices, keys, claims, certificates, invalid claims, privacy stings, profile etc.

Shared between participants

- Records all changes across smartphones
- Participants have own copy through replication
- Permissioned, so participants see only appropriate transactions
- Shared system of record

5.1 Consensus Protocol

A consensus protocol has three key properties based upon which its applicability and efficacy can be determined.

1) **Safety**: A consensus protocol is determined to be safe if all nodes produce the same output and the outputs produced by the nodes are valid according to the rules of the protocol. This is also referred to as consistency of the shared state.

Diro achieves a shared consistent copy across nodes for relevant directories using continuous synchronization and elapsed time based conflict resolution.

2) **Liveness**: A consensus protocol guarantees liveness if all non-faulty nodes participating in consensus eventually produce a value.

Diro produces highly usable contact directories with eventual consistency based on lazy consensus. There are plans to incorporate proof-of-importance to make it safer.

3) **Fault Tolerance**: A consensus protocol provides fault tolerance if it can recover from failure of a node participating in consensus.

Diro remains fault tolerant as it is not dependent on centrally stored data or any particular node. Any directory gets automatically resurrected from other nodes.

Other properties

Blockchain type: Permissioned - any user can download the directory client to create an account and join the network but needs permission or validation to participate and drive consensus.

Transaction finality: Lazy consensus

Transaction rate: High number of simultaneous transactions

Cost of participation: None

Scalability of peer network: High with sub-networks.

Trust model: Semi Trusted with incremental consensus and priority to youngest orphans.

Orphaned blocks are blocks that were included on the temporary forks created off the main blockchain. The node producing the uncle block and including it in the blockchain is given a reduced reward to encourage such nodes to always continue with the latest blocks in the blockchain.

5.2 Decentralized LDAP and Multi Factor Authentication (MFA)

Enabling contact directories as dLDAP
Lightweight Directory Access Protocol (LDAP) version 3 is now the most widely used and accepted open standard under RFC 4510. It is adopted by over 90% fortune 500 companies (using AD). Most IAM vendors support the protocol and open source having multiple projects having production grade servers in use. The primary benefit of LDAP is the provide user directories with common authentication for organizations across different applications. Offering LDAP on contact directories reduces redundancies and eliminates provisioning workflows, admin and group management. Further LDAP servers being critical for access to all company applications pose a central point of failure. Building redundancy and backups itself is a chore that small companies avoid at the cost of data security.

Using Mobiles for password less MFA experience
A study by research firm Gartner shows that 95 percent of Web app attacks make use of stolen passwords. The LDAP system may further redirect the authentication to mobile with simple confirmation. The mobile notification may be configured to further require signing with private key and manual user acceptance to validate a login request on cloud services.

OpenID Connect for exchanging identity information
SSO is important but needs to bridge across SSOs. OpenID Connect (OIDC) (OpenID Foundation, 2017) is a simple identity layer built on top of the OAuth 2.0 protocol, which allows clients to verify the identity of an end user based on the authentication performed by an authorization server or identity provider (IdP), as well as to obtain basic profile information about the end user in an interoperable and REST-like manner. This could easily be added on top of dLDAP.

OpenID Connect is increasingly the common authentication protocol. When an app prompts you to authenticate using your Facebook or Google+ credentials, the app is probably using OpenID Connect. It is easier to integrate than SAML, and it can work with a wider variety of apps.

LDAP and MFA are protocols that can be implemented on top of contact directories using mobile devices as mobile authenticators. The contact directories can act as Virtual Directories and user store for other LDAP based authentication and authorization.

6. Using cryptography and blockchain to decentralize Identity

Federated Identity and entitlement is a key part of distributed architecture. As the world is gradually moving towards ambient computing, the physical world will seamlessly merge with the digital world to create next-gen UX based on augmented reality, virtual reality & IoT devices. Trustless identities are needed for security & context for enabling this next-gen digital engagement & smart contracts (Active Contacts- dApps). Further, universally reliable identities provide accountability in the digital world while making regulatory oversight possible. By having accountability across the ecosystem through reliable identities, Diro solves multiple issues like theft, corruption, tax evasion or fraud.

By definition a digital identity is
"a globally unique identity[a]; non-synthetic[b]; singularly representing a living person[c]; having irrevocable ownership[d]; and control over one such identifier[e]."

a) a globally unique identity;
   - Must not change and associated with a public set of keys.

b) non-synthetic;
   - Should be globally unique based on social graphs and human confirmation.
   - Impossible to create without daily human interactions.

c) singularly representing a living person;
   - The identity must be used regularly.
   - Must not be ghost used and have live human confirmation.

d) having irrevocable ownership;
   - Impossible to loose ownership or access.
   - Possible to regain control of identity in all circumstances.

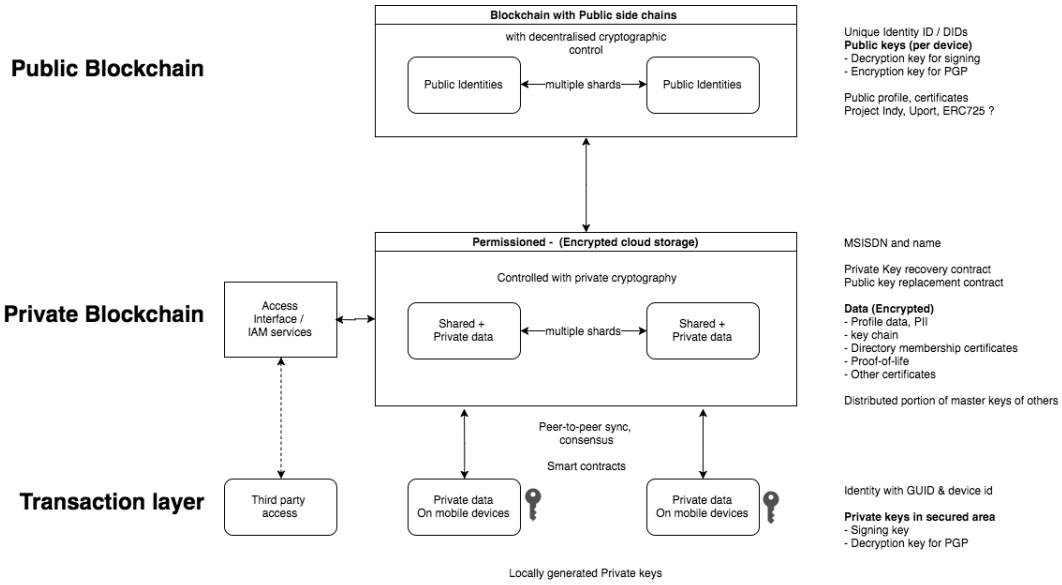
e) and control over one such identifier.
   - recycle /revoke public keys or devices.
   - Needs to be almost unhackable and even then recoverable

Digital Identity has three aspects:
Proof of global unique identity
    Consensus driven latent identities
    Social contacts grid based on consensus
    Non-duplicate and global
Proof of aliveness
    Continuous chain of social interaction
    Human confirmation (through deep interaction like audio / video)
Fault tolerance
    Manage identity theft/attack using consensus of social interaction
    Key management and recovery
    Managing decentralized consensus between nodes

Further decentralizing the identities has four key challenges

Managing and securing the Keys
1. Changing the Public Key in case of compromise
2. Safely recovering the Private key when lost

Validating and authenticating the identity
3. Validating if the identity is not synthetic
4. Validating if the digital identity is being used by the right person



Because DIDs reside on a distributed ledger, each entity may serve as its own root authority—an architecture referred to as DPKI (decentralized PKI).

Public blockchain

Contains immutable decentralized Identity data replicated across n nodes with public keys. A DID is maintained for every Identity created based on the MSISDN. (W3C community group, 2017)

Private blockchain

Contains encrypted backup of all digitally signed blocks generated on mobile devices having distribution permissions. It's the sync layer between multiple Identity linked devices for distribution of blocks or JSONs that may contain smart contracts.

Transaction layer

The nodes may also be identity hubs containing Identity data. Each node can generate blocks that are then independently verified by other nodes based on the distribution of the block. The multiple verifying nodes may together revoke the public key of the originating device if a block is found to be malicious or a device is found to be compromised.

The master key is directly sharded and encrypted at the local device with PGP key of other trusted devices. Can use Shamir's secret sharing (SSS) or threshold signatures to generate and later combine the shards of master key.

6.1 Using Smart Contracts to manage the Public Key

uPort has recently suggested a method to decentralize the maintenance of public keys by the identity owner using blockchain and smart contracts. The purpose of having a Proxy contract as the core identifier is that it allows the user to replace their private key while maintaining a persistent identifier (uPort). If the user's uPort identifier instead was the public key corresponding to their private key, they would lose control over their identifier if they were to lose the device where the private key is held. (Lundkvist, Heck, Torstensson, Mitton, & Sena, 2017)

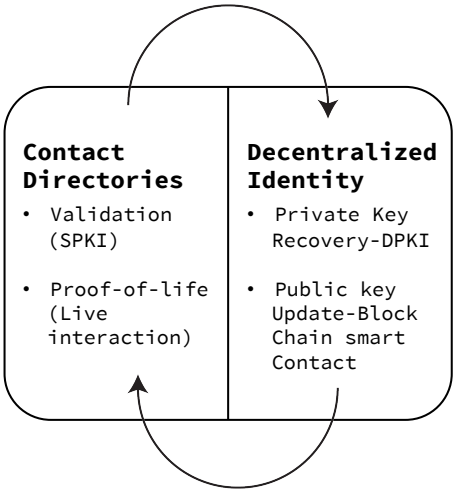
Thus having a persistent ID that can have a replaceable public key and private key set makes owning the identity easier and safer.

6.2 dPKI for recovering private keys

Decentralized identity data needs secure cloud storage that can be recovered in case of data loss. The data includes certificates, profile attributes etc that would need encryption.

The encryption itself could be symmetric and the key needs to be backed up for recovery. Any central storage of such keys would render the whole system vulnerable and defeat the original objective of decentralization. The problem was aptly identified and solved by members of rebooting-the-web-of-trust using a group based recovery scheme.

The security and usability problems of DNS and PKIX can be addressed through the use of decentralized key-value data stores, such as block chains, to create a specification for a Decentralized Public Key Infrastructure (dPKI). In describing the properties of dPKI, it works even on resource-constrained mobile devices, and that it is able to preserve the integrity of identifiers by protecting organizations and indivdials from private key loss or compromise. (Allen, et al., 2015)



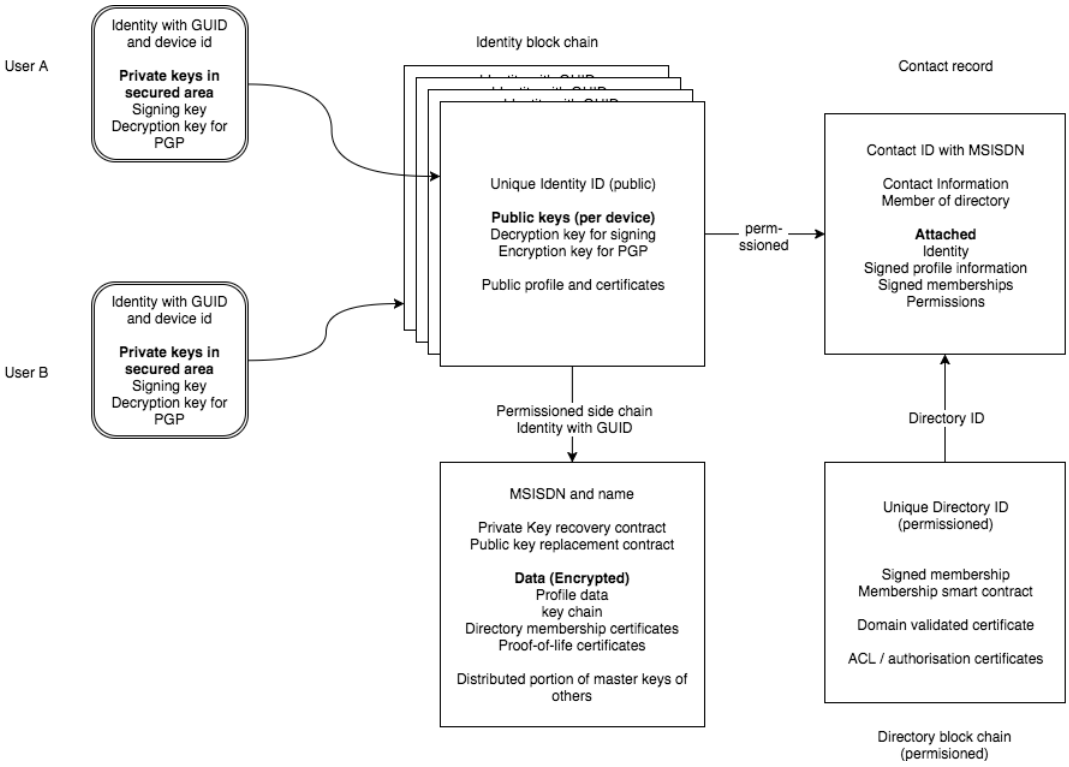
6.3 SPKI to sign identity data to validate identity

Digital identities need to be certified by other agencies or social consensus to become more reliable. SPKI offers a decentralized model to issue such certificates and authorizations within the directory framework. SPKI offers a special opportunity to strengthen the social fingerprint (Carl Ellison, 1996). It makes identities within contact directories trust worthy by third parties. A person may be certified through multiple directories and the social graph of mobile numbers in a decentralized architecture similar to a Web-of-trust. A unique identity is generated using SPKI without a name and bound to an active MSISDN along with a globally unique identifier (GUID). These certificates can be easily discovered using directories or MSISDNs. (Ellison, 1999)

. The directories can be domain verified using email verification or better still signed using a domain validated certificate.

LDAP enables the public keys of users and certificates to be accessible by other third parties.

Diro platform issues new signing & PGP key for each new device used by the Identity. The Identity data is secured using PGP. The contact data narrow casted is signed by a private key of the user. The directory changes are further authorized using digital signatures of contributors and validated with architecture similar to smart contracts.



The SPKI system allow the platform to have decentralized control secured by billions of private keys and central certificate authority.

6.4 Cryptographic KYC

A digital identity may be validated by a browser that is enabled to capture the SSL certificate along with the web page displayed along with the time stamp as a hash on the blockchain. These claims can prove ownership to a bank account or a utility service with cryptographic validation through the SSL certificate captured. (IN Patent No. Universal original document validation platform , 2015) This can eliminate the need of citing original documents and linking it the Identity owner by needing to see him in person. Further this is more credible as the original documents can be tampered while the web capture can be cryptographically trusted. Allowing such remote KYCs once and adding it as a verified claim could make the whole KYC process frictionless.

6.5 Validating authentic digital identity owner with proof-of-life

Smartphones offer a unique opportunity in validating identities using live social interactions. These live human voice and video interaction give us a passive way to eliminate synthetic identities and defend against Sybil attacks. An identity trust score can be easily built for privilege access using such human validations that are more secure than any biometric systems. When users have a live conversation with other members in their social groups and across different groups it generates proof-of-real person owning the device and thus acts as a real bridge between physical and digital identities.

Authentication levels

1. User identified with one-time password
2. User authenticated with social fingerprint using directories
3. User previously confirmed by having live conversations
4. User transaction confirmed by subsequent live conversations

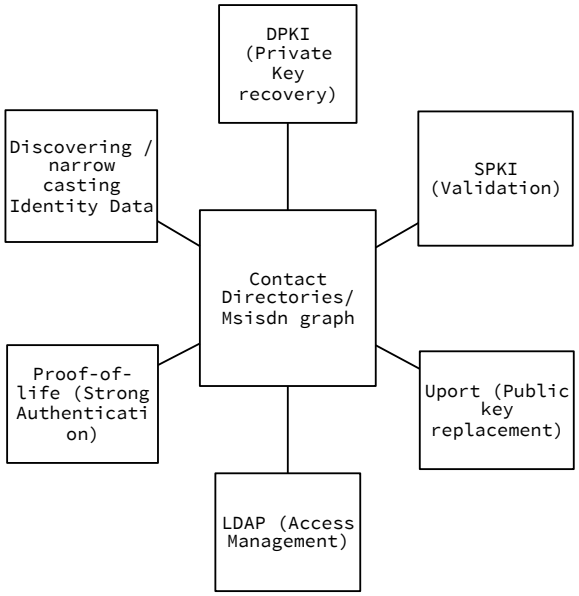
Any private and public key changes or retrievals could be limited to Level 4 authentication. These authentications would ideally be done on a smartphone dialer app that supports live conversations with other devices to obtain a mesh of such confirmations from them. The confirmations could be explicit or implicit. The implicit confirmations may be based on length of the conversation using voice or video.

The user, on sign up, may select a list of individuals to validate his/her own identity based on interactions. On specific interactions, the trusted members would then digitally sign the device as authentic for a short period. The user may then declare authorization level before signing transactions based on collected signatures and share with trusted devices. In case of incorrect declaration, the trusted devices could revoke the signing key of the user.

7. Conclusion

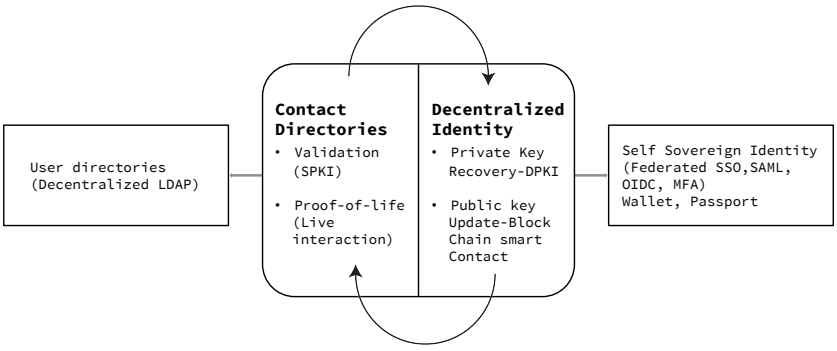
Contact directories offer a rapid method to validate digital identities using SPKI to do social KYC. It further offers a possibility of strong identity authentication through live interactions with human confirmations over voice and video calls. Voice and video conversations offer a continuous stream of strong authentication to digital identities.

Further, a decentralized identity platform requires a safe public & private key management and recovery process to make owning identities possible. The DPKI and uPort based architectures also require social proof for key management and recovery. Therefore, social KYC is a critical factor for authentication across different aspects of creating a decentralized identity structure including key management, identifying non-synthetic identities and generating proof-of-life authentication from other devices.



Contact directories based on MSDINs open up a new realm of decentralized identity and access management infrastructure across multiple domains like web, apps, blockchain, AR/VR & all other industries as user directories for context and security (LDAP).

Crowd sourced contact data containing MSDINs offer a rapid source of building a universal decentralized identity system that is a holy grail for delivering public benefits.



Scaling trust with block chain
Identity and security for establishing trust are critical building blocks on blockchain. Contact directories or social graphs are a central component in decentralizing the identity and access management. Without using social confirmation building a reliable decentralized identity and security architecture is not possible.

8. Works Cited

Vinay Gupta. (2017, July 7). *A Blockchain Solution For Identity?* Retrieved from Medium: https://medium.com/humanizing-the-singularity/a-blockchain-solution-for-identity-51fbcae94caa

Gartner. (2016, Oct 13). *2017 Planning Guide for Identity and Access Management.* Retrieved from www.gartner.com: https://www.gartner.com/binaries/content/assets/events/keywords/identity-access-management/iame11/2017-planning-guide-for-identity-and-access---13oct16.pdf

OpenID Foundation. (2017, 11 15). *openid.net*. (OpenID Foundation) Retrieved from openid.net: http://openid.net/connect/

Allen, C., Lundkvist, C., Nelson, J., Reed, D., Sabadello, M., & Slepak, G. (2015, December 24). *Decentralized Public Key Infrastructure.* Retrieved from Github: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/dpki.pdf

Carl Ellison, C. I. (1996). *Establishing Identity Without Certification Authorities (1996).* Retrieved from CiteSeer: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.31.7263

Ellison, e. a. (1999, Sep). *SPKI Certificate Theory* . Retrieved from Network Working Group - IEEE: https://www.ipa.go.jp/security/rfc/RFC2693EN.html

Gupta, V., & Rai, N. (2016, Mar 2). *IN Patent No. PCT/IB2016/055271.*

Lundkvist, D., Heck, R., Torstensson, J., Mitton, Z., & Sena, M. (2017, Feb 21). *uPort: Platform fo Self-Sovereign Identity.* Retrieved from Uport.me: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf

ID2020.org. (2016, July 1). *Identity 2.0*. Retrieved from ID2020: http://id2020.org/news/2016/12/2/identity-20

Gupta, V. (2014, Mar 9). *USA Patent No. PCT/US2015/019443.*

Vishal. (2016, Mar 16). *IN Patent No. PCT/IB2017/051056.*

W3C community group. (2017, Nov 30). *Decentralized Identifiers (DIDs) v0.7.* Retrieved from Github: https://w3c-ccg.github.io/did-spec/

Reed, D. (2017, Sep 30). *Architectural Layering for Decentralized Identification.* Retrieved from Github: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/Architectural-Layering-for-Decentralized-Identification.md

Gupta, V. (2017, Jun 19). *IN Patent No. PCT/IB2017/053622.*

Gupta, V. (2015, 05 27). *IN Patent No. Universal original document validation platform* .