Whitepaper

v1.3

Team Hypersign

https://hypersign.id

Problem of consumer facing application

The Consumer Identity & Access Management market is growing rapidly, spurred by the widespread adoption of 'mobile' and 'Internet of Things'. Allied Market Research reports shows that this is driven by smartphone adoption: Growing popularity of mobile devices and flexible functionalities of consumer IAM solutions to tackle increased network traffic, burgeoning demand, and peak usage requirements of consumers for various applications are expected to supply numerous opportunities for the expansion and development of the worldwide identity and access management market.

Most customer-facing applications rely on either third party authentications like OTP based authentication or social logins such as Facebook, Google and the likes.

OTP [One Time Password] Logins

OTP based authentication, at first, seems to be a better solution (widely accepted within the enterprise) when compared to social logins, as it provides some sort of guarantee to service providers that the user actually possesses the phone number or device - the answer to the 'What you have?' question (i.e. Proof of Possession) - since it is not viable for a user to share his mobile device with another person. But this guarantee comes with a cost for both the service providers and the end-user.

Insecure Channel

The OTP is based on SMS channels which cannot be considered secure. Two reasons contribute to this fact. First, the security of SMS OTP relies on the confidentiality of SMS messages that successively relies on the safety of cellular networks. Lately, several attacks against GSM, and even 3G networks have shown that the confidentiality of SMS messages cannot necessarily be provided. In addition, in some countries like India, cellular network traffic is not encrypted by default, mobile network operators disable wireless encryption of SMS and call traffic to decrease network load.

Wireless interception, Trojans, SIM swap attacks

An Attackers goal is the acquisition of a users OTP, for which they employ multiple creative ways to get a hold of a user's OTP, such as wireless interception due to lack of mutual authentication and weak encryption algorithm, mobile phone trojans such as ZITMO - specially designed to intercept SMS messages containing OTPs, SIM Swap Attack where an attacker tries to get OTPs on SIM they posses, etc. Reasons for these

kinds of possible attacks can be many, such as “cellular network insecurities”, “mobile phone design issue”, “lack of awareness of data privacy” amongst others.

Users hesitation in sharing phone numbers

The ‘phone number’ can now be considered as a critical attribute of user identity since it is all linked to bank accounts and other sensitive products and services. If a user wants to try a service in order to check its befitting, the user must share multiple attributes of their identity along with the phone number with an entity with which they might not want to keep a long-term relationship.

“The fear that a phone number can be misused by this entity which the user does not trust.”

Users want to keep their personal data safe and private; especially their phone number and only share it with people and companies whom they fully trust. Once a number gets shared widely, potential problems arise, such as unwanted messages, spam calls, and more.

Phone number is not enough

Apart from capturing the phone number, service providers ask users to provide additional personal data in order to build a customer profile in their applications, since OTP authentication only verifies a user’s phone number, but not other details such as email, name, address, geolocation etc.

OTP is sharable

The ability to share an OTP (even under its “time to live” period) makes it as bad as username and passwords which not only violates the principle of “Proof of possession” but also makes it highly vulnerable for many possible attacks. According to a recent survey by OLX: 26% of Internet-users said that they have shared sensitive OTPs (one-time pin/passwords) with others.

Used as second or multi factor

Although it seems like OTP answers the question of ‘What I have?’, but still does not answer the question of “Who I am?” - meaning that the OTP is always used as a second factor since it does not give enough confidence to verify who exactly the user is. Being used as a second or a third factor authentication medium, it greatly affects an users experience to access services. Moreover, the OTP-messages are often delayed or lost or end up in spam folders and this greatly affects the overall user experience and potential loss in business due to failed logins.

“The OTP is based on SMS channels which cannot be considered secure. Moreover, end users do not feel comfortable sharing phone numbers since phone numbers have become critical pieces of personal information.”

Social login

The social login helps service providers to quickly onboard a user without requiring them to go through the registration process. This way, on one hand the service providers are able to provide seamless onboarding to their user and on the other hand users do not need to type their personal information like name, email, phone number, every time they need to access a service. Moreover, the pain point of having to remember multiple usernames and passwords for each of these services is also eliminated. Finally, the service provider also gets the user data from the social login provider (also called identity provider, i.e. IDP) in order to build a customer profile.

There are multiple challenges with social login authentication;

Legacy Authentication

Most of the social logins providers like Facebook, Google, etc. still rellies on a password based authentication and the problems with this archaic mechanism are quite notorious such as password resets, password hacks, forgetting passwords and more.

When a user tries to access a service through Social Logins, this is a major risk for the Service Provider. If the user cannot log due to any password related issues, this is a direct loss of business for the service provider, as users will be unable to use their services.

Central Storage

The identity provider stores data of millions of users centrally. This centralized database becomes a honeypot for hackers.

We have seen many cases related to identity theft and userdata issues. This is a serious problem for users who are concerned about data privacy and protection as they have to fully trust these IDPs on how they store and manage their personal data.

Data misuse

The identity provider holds the power to misuse the user data without consent in different ways, such as, tracking, tracing, running analytics, or even just by selling this data to someone else.

Tracking and tracing

Social login providers can track a user based on where they are logging into -

“Facebook would know if you are buying a ticket on MakeMyTrip or buying something from Amazon!”.

This creates privacy concerns for users. Finally, using the username - password mechanism over a social login never really proves the basic questions required for proper identity verification which are ‘What you have?’ (i.e. Proof of Possession) or Who you are? (i.e. Proof of characteristics).

Too much trust

Both end users and service providers are forced to trust the IDPs on how they store and share personal user data.

“There are many problems we analyzed with social logins, such as storage of user personal data, tracking & tracing, data misuse, legacy authentication using passwords that require too much trust.”

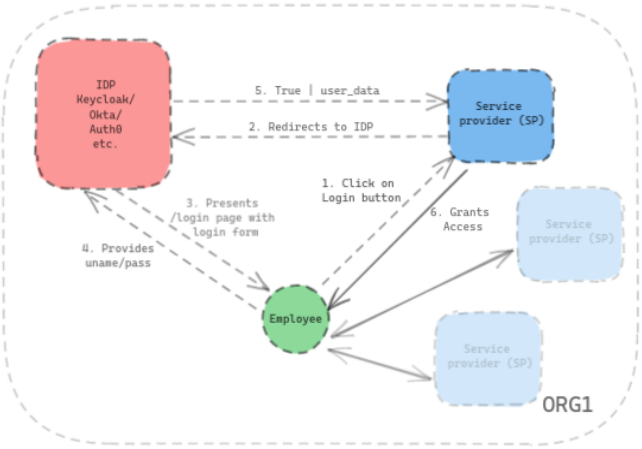
Problem of employee facing applications

Passwords are weakest link

A recent survey of U.S. companies found that each employee costs an employer average of $420 annually just grappling with passwords. With 37 percent of those surveyed, were resetting their passwords more than 50 times a year. The losses add up quickly, in productivity as well as the cost of the support staff and the help desks. Lastly the financial burdens are even bigger. As mentioned earlier, passwords can be easily shared and therefore are the weakest link.

Expensive

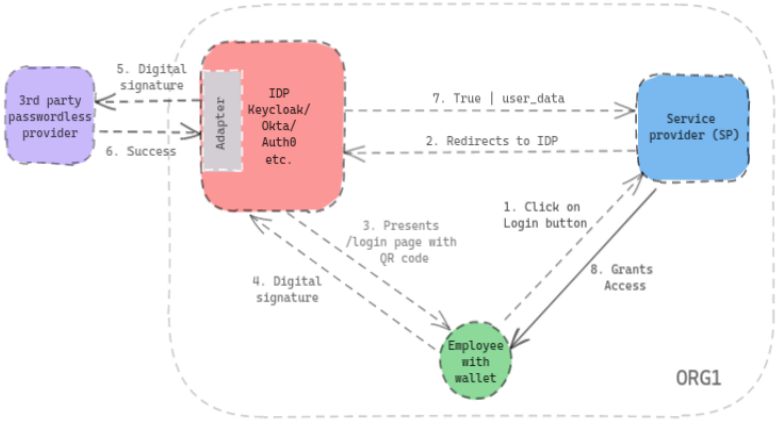
Enterprises would like to run their own IDPs system and not trust any third party provider. This not only helps them to get control of their employee data, but also helps them to drastically reduce the overall cost of passwordless IAM solutions. In order to disrupt the Identity management industry, the main challenge is to provide “better security” at an “affordable cost” to an enterprise. Although this is fairly simple to achieve from a technology perspective, on the business side there are large corporations trying to consolidate control.



For Example, major corporations (Cisco, Microsoft, Gemalto/Thales) charge customers an exorbitant fee for all these products and features. On the other hand, Facebook and Google who literally provide all the authentication and authorization services for free but at the cost of violating user data privacy, hence cannot be trusted by serious enterprises who are very much concerned about their employee data.

The current IAM solutions, like Okta, Keycloak, Auth0 etc., in the market can cost upwards of $30,000 annually, which may be very expensive for small and medium enterprises who want to have decently secure but cost effective IAM systems for their employees.

Moreover, converting username and password based legacy systems into passwordless solutions by adding a centralised 3rd party provider, like FIDO, OTP, etc. will not just further increase the overall cost of an already expensive solution but also increase the trust on these external entities. See the figure.



That brings us to 3 major problems for any enterprise;.

- It restricts the market to only the highest-value credentials. (Only the rich can have better security)
- It favors the largest providers who are the biggest targets for data breaches (e.g., Equifax).
- It prevents the use of powerful new privacy preservation technologies like selective disclosure that could further protect personal data.

Access from unsecured environment

A number of companies who have previously adopted the centralised and legacy based IAM solutions are now starving for better security, especially during this COVID pandemic where work from home has become ‘the new normal’.

On one hand they can not remove the existing system and implement a new solution as they might have already paid for those service, however on the other hand they now also need to ensure that those who are logging onto the system [remotely] are actually their employees Given the fact that legacy credentials like username and password (including OTP) can be easily shared since employees are not working from secured environment like offices. Security threats have gone all time high during the pandemic.

Moreover, the WFH setup is going to be standardized in the future since it has brought much convenience and cost effectiveness to business. Many companies have already adopted full time or partial WFH setup. Therefore, not only is a passwordless identity and access management solution the need of the hour, deploying it quickly to the masses is also imperative.

Federation is complex

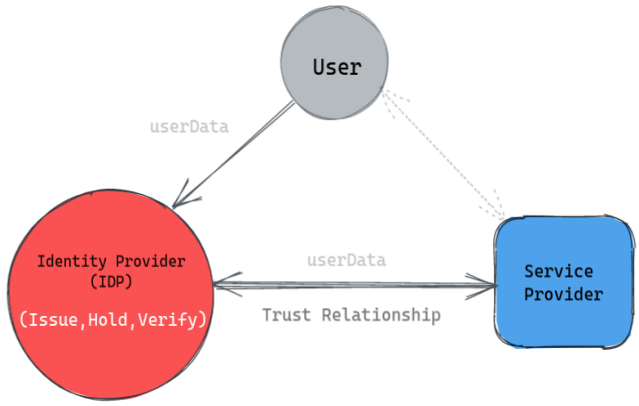
Federated in identity and access management is an arrangement that can be made between multiple enterprises to let employees use the same identification data to obtain access to the applications of other enterprises in the group.

A very common protocol to achieve federation is SAML 2.0. Virtually all of the cost of SAML 2.0 Single-Sign-On projects are labor-based. Costs often are unplanned and grow to become excessive as companies underestimate the scope and complexity of a SAML implementation. An enterprise might have to spend anywhere from 2-12 weeks, or 80-480 working hours, to deploy an initial SAML implementation. This is certainly a problem for small and medium enterprises.

“Most enterprise IAM solutions are complex to implement, manage and impose a very high TCO [Total Cost of Ownership]. Additionally, they still offer legacy authentication mechanisms using usernames and passwords, which increase the risk of breaches and hacks drastically”.

Current Identity and Access Management

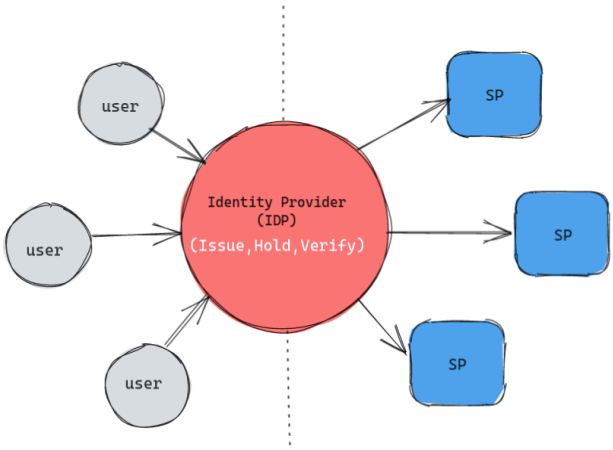
Now that we have understood the problems associated with consumer facing IAM and employee facing IAM systems, let's understand the implementation of current systems before we address the solution.



When A user shares personal data with an IDP; the IDP then issues a username and password as a credential. This is the only information the user keeps with himself. Whenever a user wants to access the SP, the IDP verifies the user credentials and shares his personal data with the service provider, upon successful verification.

Notice in the above figure how the trust-relationship is strong between SP and IDP and also how users do not control their own data.

In the current model of identity systems, the IDP sits in the center of the ecosystem and is responsible for credential issuance, holding and verification. This gives the IDP the full control and access to user data.



Problem summary

Service provider (SP)

- SPs have to fully rely on high availability, security and scalability of identity providers.
- The SP does not know how their users' data are being stored and managed by these IDPs.
- In the case of OTP based authentication, verifying a phone number is not enough to build a user profile. Moreover, the security of SMS channels is always in question.

- Many end users are reluctant to provide their phone number as it can now be considered a critical attribute of user identity since it is linked to bank accounts and perhaps other sensitive government related services.
- Monopoly of IDPs raises the cost of IAM solutions.

Identity Provider (IDP)

- The identity provider has to manage millions of records which become honeypots for hackers.
- As the number of online services grows, the number of verification requests will grow exponentially. This can stress out the issuance systems and lead to downtime for critical processes of authentication.
- IDPs such as social login providers, do not confirm the user who is actually using the credentials to log in, as the credential can be easily shared with peers and used by others.

End user

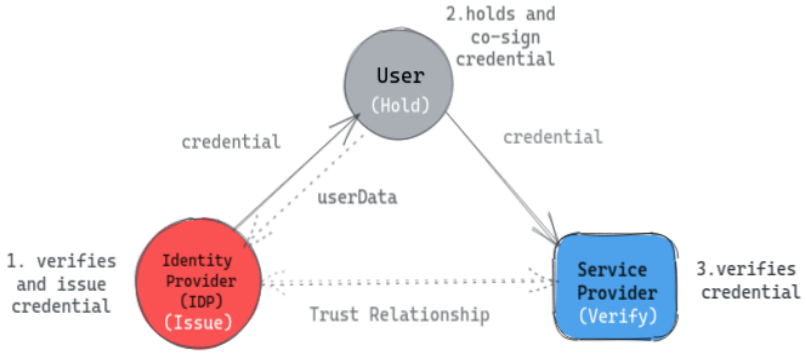
- Users have no control on how and when their data is being stored, managed and shared by the identity providers.
- In case of OTP they have to go through a hustle of filling their user details every time they onboard into a a new service.

“In current identity systems, the IDP sits in the center of the ecosystem, making it a critical and trusted entity. Putting too much trust in one system is a problem.”

Hypersign

Hypersign is a decentralised identity and access management infrastructure for the enterprise. It leverages technologies such as public key infrastructure (PKI) and blockchain to provide passwordless authentication as well as authorization and verification services which integrate within minutes and is compatible with legacy IAM systems at an affordable price-point.

The Hypersign works on the concept of Issuance-verification paradigm where we essentially have three stakeholders.



Users: Access services and hold their own personal data [End Users].

Issuer: The one who verifies user-data and issues credentials based on user-data. I.e identity provider.

Verifier: The one who verifies credentials. I.e service provider.

The Hypersign protocol distributes the responsibility of issuance, holding and verification among stakeholders. In the above figure, the user gives personal-data to the issuer, which verifies and issues a cryptographically signed document (verifiable credential) to the user.

The verifiable credential contains user-data along with the digital signature of the issuer. At this stage the issuer need not to store user-data and can act as a stateless server. Optionally, Issuer can store data in encrypted form for recovery or future access.

The end-user can store the verifiable credential in any user-agent such as a mobile device or cloud agent which only they have access to. This gives the end-user the ability to control their own personal data.

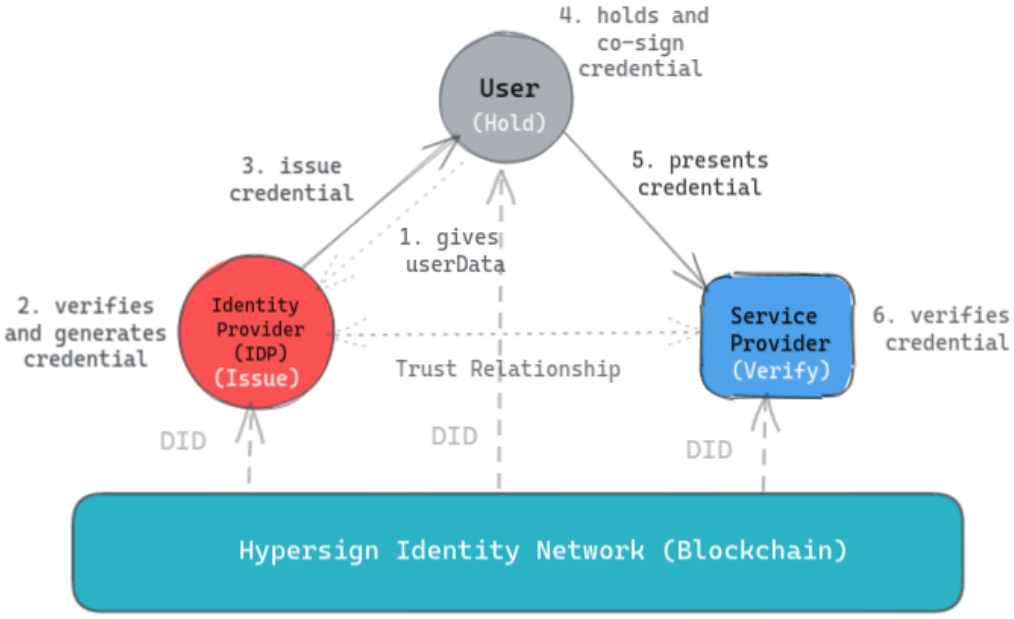
The user can now present this credential to the service provider, in a peer-to-peer fashion without notifying the identity provider or the issuer, whenever they want to use a service. This gives the end user a sense of privacy. Before sharing the verifiable credential, the end-user also attaches his digital signature on the document.

The verifier or service provider can obtain user-data from the verifiable credential and can verify digital signatures of the user and the identity provider. The multi-signature mechanism is to ensure that not just the right issuer but also the right owner of the document. Furthermore, the digital signatures also ensure the integrity of the document. The credential presented by the end-user can be verified by the service provider independently - without making a verification request to the issuer or IDP. This helps SP to scale the system as it need not to require the IDP to be available online at the time of verification.

Independent verification using blockchain

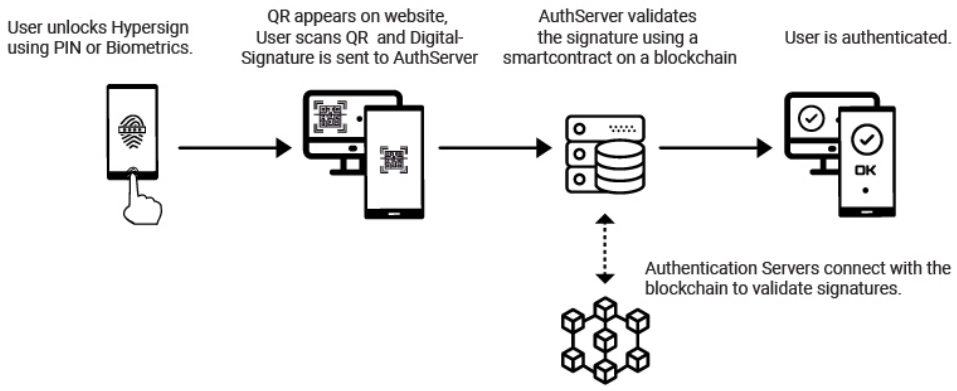
Although service providers in the Hypersign ecosystem trust the Issuer, unlike legacy systems, the verifier need not to rely on the issuer or the IDP to be available online for verification of credentials given by the user. This means that the verifier can verify the credential on its own.

Blockchain plays an important role in the Hypersign ecosystem. The Hypersign protocol uses blockchain for global tamper proof registry of public keys. Blockchain gives ability to all actors to verify digital signatures of each other on their own.



In order to verify digital signatures of the issuer and the user, the verifier queries the blockchain with respect to an identifier also called decentralised identifier aka DID, and fetches public keys. Now these public keys are used to verify digital signatures. The procedure of independent verification helps to scale the overall system.

How does it work?



The Hypersign protocol works in three steps:

ONBOARDING ACTORS

Users, Service Providers and Identity Providers register on the Hypersign Network

1

CREDENTIAL ISSUANCE

User requests credentials from Identity Provider, Identity Provider verifies the user data and issues a signed credential

2

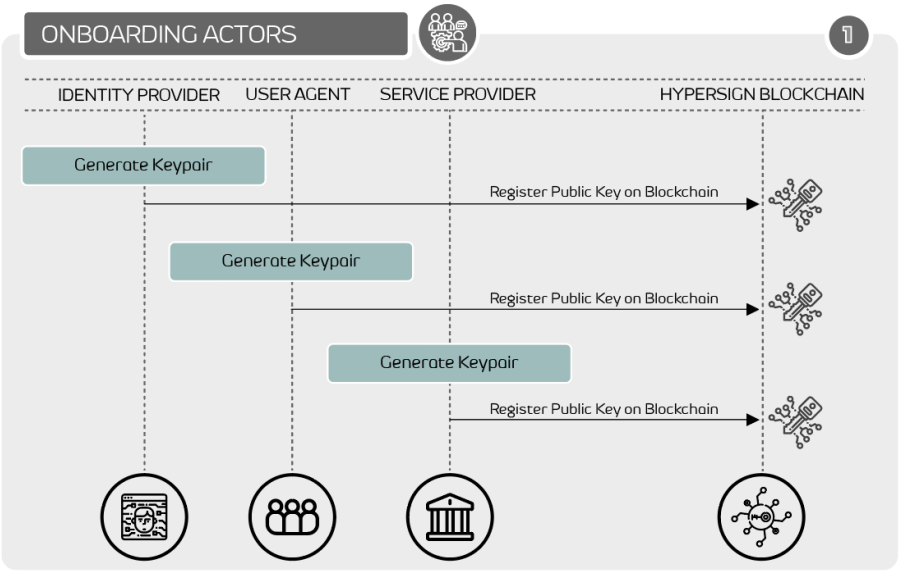
REGISTRATION & LOGIN

'One Step' User Registration & Login, by providing credentials to Service Provider. The Service Provider verifies signature of user and Identity Provider on Hypersign Network

3

Onboarding Actors

First, all actors (Users, IDP and SP) need to be on-boarded on the Hypersign Identity Network. On-boarding is the process of registering public keys on the Hypersign network. Once an onboarding request is made, the blockchain stores their public key and issues them an identifier called, decentralised identifier aka DID. Moreover, one can also store information other than the public key which he might want to make public. For example, a bank can store the website url, address of the bank, IFSC code, etc. Take a look at the figure below.



Credential Issuance

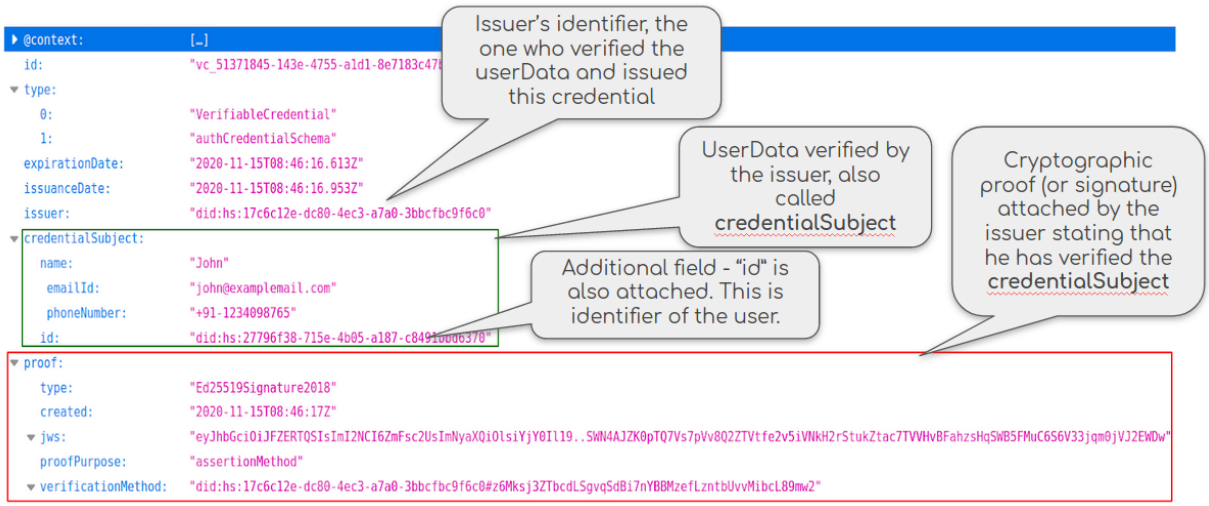
Once all actors are onboard, the next step is Credential Issuance.

In this step, a user requests the verifiable credential from an Identity Provider by providing his data. The user data can be anything from email, phone numbers to address, geolocation, IP, and so on. Take a look at one simple example, user-data in the figure alongside.

```
{
    name: "John",
    emailId: "john@examplemail.com",
    phoneNumber: "+91-1234098765"
}
```

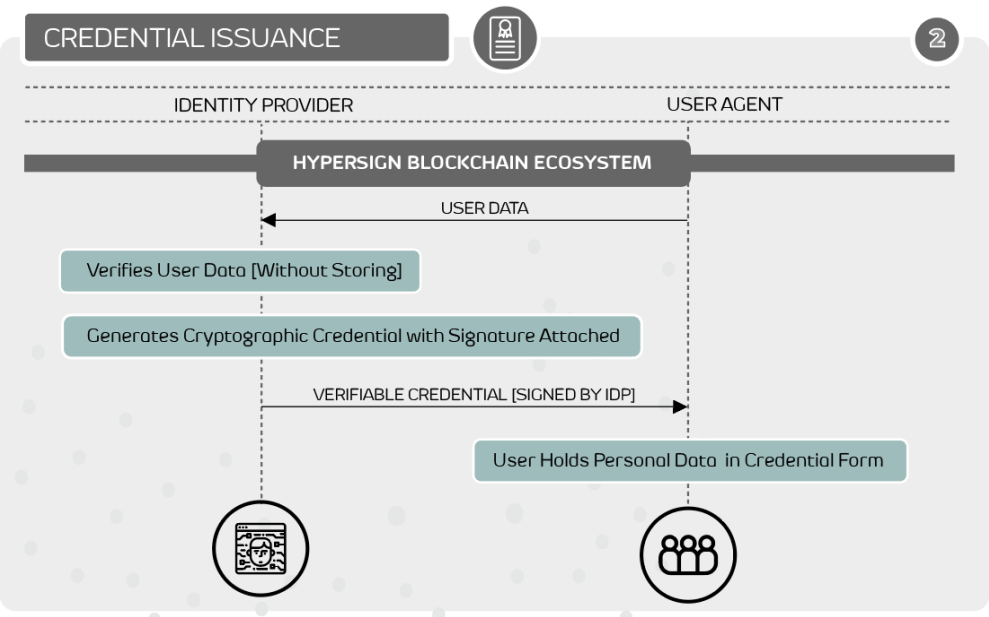
The IDP verifies this data and issues a cryptographically signed credential also called ‘Verifiable Credential’ [VC]. The VC contains verified user data, some metadata such

as issuance date, expiration date and a proof object which contains signature of the issuer along with the algorithm used to produce the signature. Take a look at VC in the figure below.



The protocol does not care about how an IDP or issuer verifies the identity attributes. For example, the IDP might want to send an email to verify the email address or send an OTP to verify the phone number - they are out of the scope of the protocol. It will depend on the use case and implementations. The user can store the credential in any user-agents such as mobile device or cloud against which is in control of the end user.

At this step, the IDP can act as a stateless server and need not to store any user-data, but just issue the verifiable credential upon data verification. This will help the IDP to not only eliminate the hassle of data storage and compliance, but also protect user data from getting hacked. The IDP can charge a fee for its service, either through external payment providers or via inbuilt payment mechanisms of the Hypersign Network [To be discussed later in this document].



The Hypersign Network also has provisions to incentivize entities, especially IDPs, to support and maintain the network and work for a noble cause.

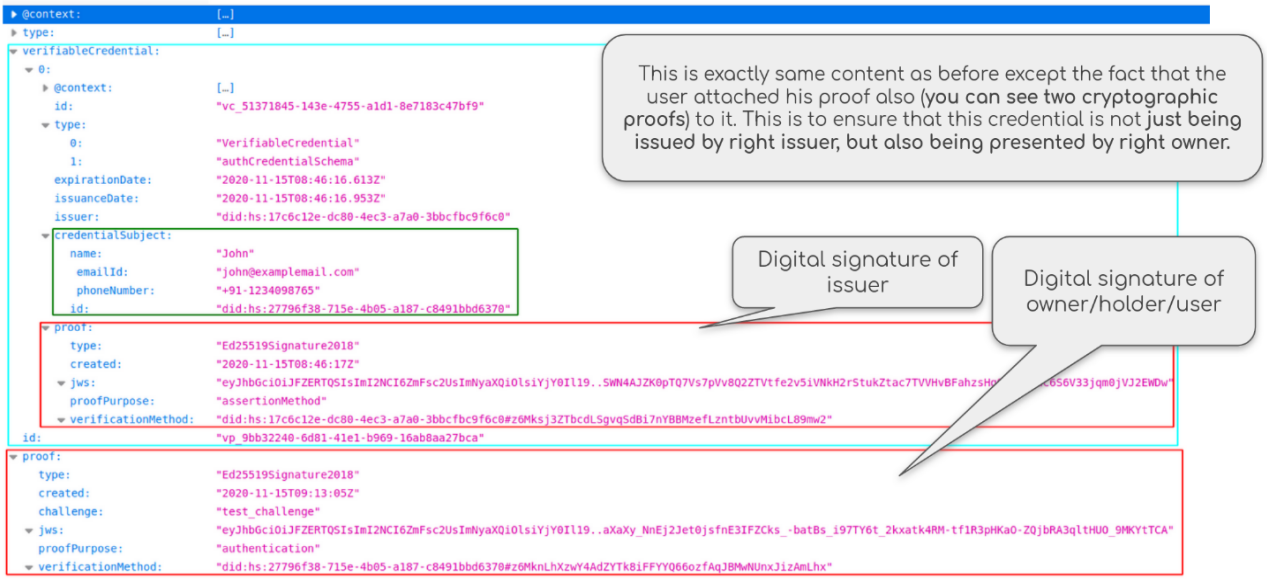
Furthermore, IDP can store these credentials in encrypted form so that the end user can recover their credential if they lose them.

One Step Registration & Login

Once actors are on board and verifiable credentials are issued, a user is now ready to authenticate himself and avail service from the service provider.

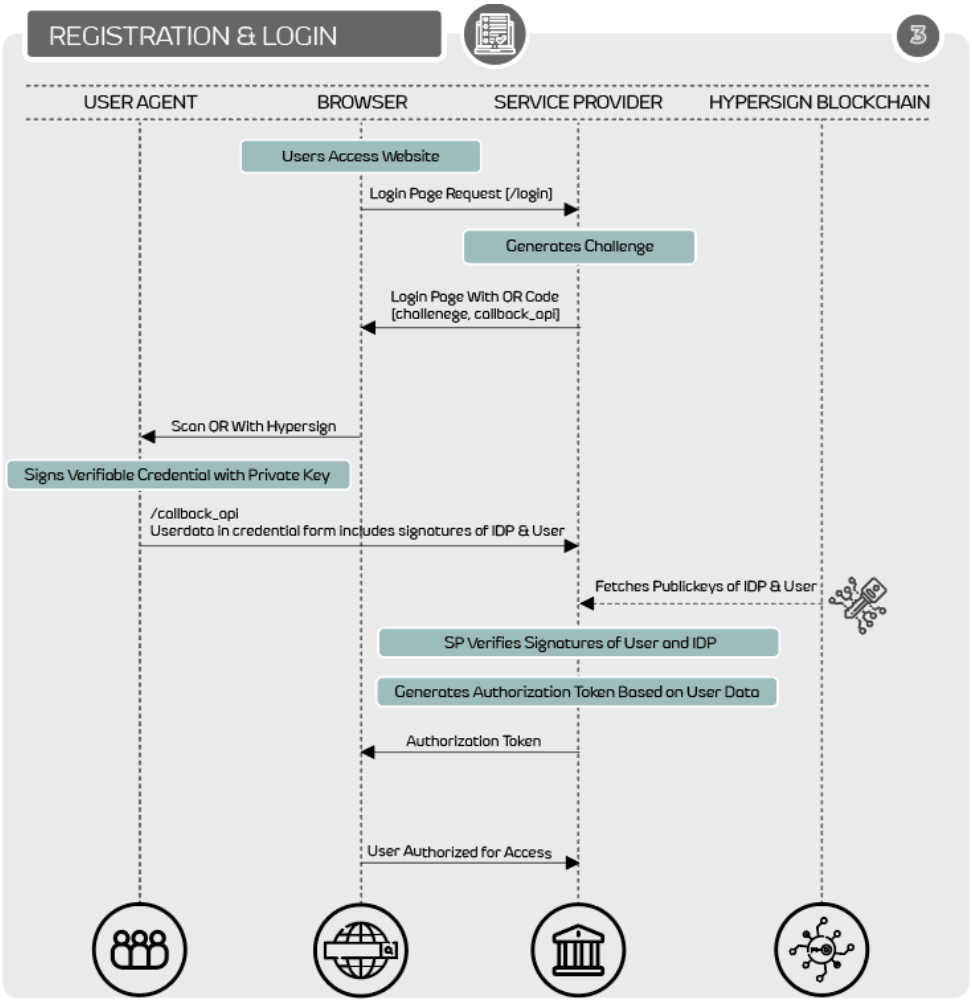
The service provider requests from the user the minimum data it needs to let them access the application. This request can be made via several different protocols, called 'DIDComm', depending on the requirement. For simplicity, we use QRCode based communication. In the QR, the SP provides its DID, a challenge, a callback API, supported credential type and data model.

A user chooses the required credential from the available list of credentials which he might have collected from different identity providers and selects the information needed for the provider. Users also have the ability to share partial data with SP. This helps to reduce excess data leakage. Before presenting the verifiable credential to the SP, the end user also signs the credential. Take a look at the co-signed credential document in the figure below.



Upon receiving the co-signed credential, the provider parses the credential document and fetches public keys of issuers and owners using their DIDs mentioned in the document from the Hypersign Network.

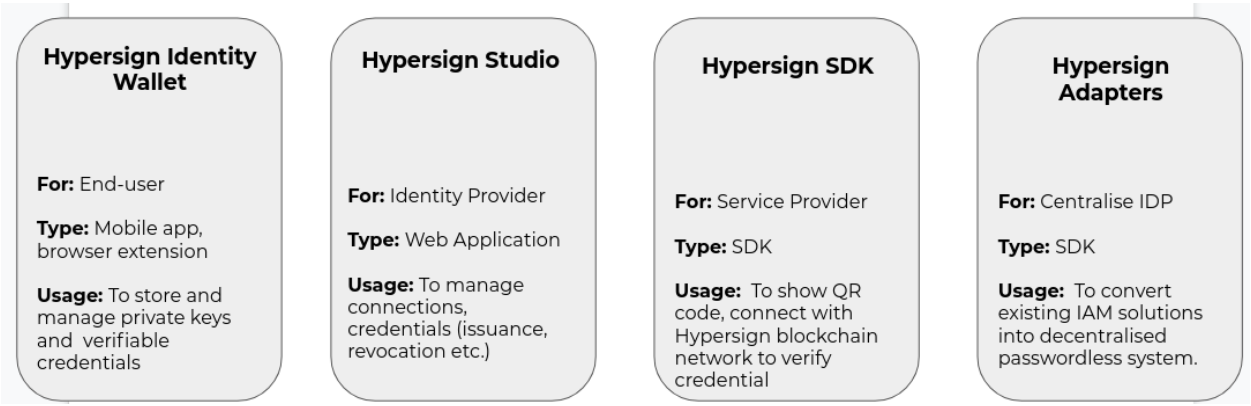
Finally, it verifies signatures and upon successful verification it generates an authorization token based on user data available in the credential document and gives access to the end user. Take a look at the detail flow in the figure below.



This whole process can be implemented with a few simple steps using Hypersign SDK. The providers do not have to worry much about implementation.

Tools and Software

Hypersign offers four main tools for any enterprise to rapidly deploy 'decentralised passwordless authentication solution' with a low TCO [Total Cost of Ownership].



Hypersign Identity Wallet

The identity is a user-agent which a user controls. It is used to hold private keys and verifiable credentials of the user. The user-agent can be a mobile app, a browser extension or even a cloud agent, depending on the use case.

Hypersign Studio

The Hypersign studio is a web based tool which can be used to manage (issue / revoke etc.) credentials by the issuer. The tool is within the Hypersign node.

Hypersign SDK

The Hypersign Software Development Kit [SDK] is a simple software which the verifier has to integrate in their website. The SDK generates the QR code on the login page and also helps to verify credentials by the service provider's server.

Hypersign Adapter

The Hypersign Adapter is a simple tool that helps to convert legacy based (username-password) IAM solutions such as Okta, Auth0 or Keycloak into a password-less authentication system. This can be used by an enterprise to provide secure passwordless authentication access to their employees. The adapters are quick and easy to integrate.

Hypersign Blockchain Network

The Hypersign Blockchain Network is the heart of the Hypersign identity ecosystem. The network is primarily used as a single source of truth of, public information such as public key, service endpoint and so on.

Although verifiable credentials are not stored on chain [not even in the encrypted form], actors can connect to the network to verify other actors. The tamperproof nature of the network provides a guarantee about the public data it holds. Furthermore, the Hypersign Blockchain network is also used to incentivize actors, using its native coin - $HID, who run and manage the network infrastructure.

We will discuss the incentivization in the later sections of this document. But first, let us understand the dynamics of the Hypersign network.

Hypersign is a hybrid blockchain network built based on the AeTernity Hyperchain protocol. The Hypersign identity network has the Proof Of Stake (PoS) consensus algorithms, but relies on Aeternity's Proof Of Work(PoW) main network for providing security, hence hybrid.

The Hybrid Model

Any identity system has to be scalable, cheap, high-performing and secure since it is the fundamental right of any human being who interacts online. Identity is not a single term, it is rather, amalgamation or set of attributes and personas - one person can have multiple identities depending on their different contextual interactions in the digital world and one service provider can have millions of users; therefore, the identity system should be able to serve them all.

We are all aware of the scalability problem of PoW systems. Although they have achieved network security by burning CPU cycles in order to randomly hand the power to users depending on their computational efforts - this is a slow and costly process, which relies on having a vast and decentralized network of miners. On the other hand, while PoW solution distributes leadership based on computational power, PoS do it based on so–called stake, which in most cases means token supply. Pure Proof of Stake (PoS) solution is much more energy–efficient, but it comes with some serious issues like nothing at stake, stake grinding, long–range attacks etc.

The Hypersign network achieves security by connecting to its parent PoW network and achieves scalability by its native PoS consensus based network. The PoS solution is also fairly cost effective and high-performing for consumers in terms of transactions fees and throughput.

The consensus works on three stages:

Leader Election

A committee of few special nodes (called validators) are responsible for the generation and finalization of blocks. A randomness is used to select the committee members. The state of the parent PoW network is primarily used as a source of randomness in Hypersign PoS network which is not just reliable but also unpredictable.

A new election happens each time a block has been mined on the parent chain. The Hypersign uses a parent blockchain with finality guarantees to hold fair and provable leader elections based on the determined voting power. Candidates submit their view of blockchain to the parent chain in a commitment transaction. A commitment transaction is nothing but their will to participate in the upcoming election . The commitment consist of the following information:

- The subject of delegation on the child chain
- The block over which the delegate is going to build
- Signature of the delegate from the child chain

When it's time to elect a new leader the commitments are gathered from the parent chain alongside the next block hash and based on the delegate's voting power a new leader is elected from the set of delegates who submitted a valid commitment. The voting power depends on how much currency (or stake) is deposited by that candidate.

Based on tokens frozen in a special contract on the Hypersign - users can delegate tokens to other users. Withdrawals from the contract are delayed for some time to allow punishing malicious leaders. The top N delegates with most delegated tokens are eligible to become leaders. The voting power increases both with stake and with time of involvement.

Block Proposal

Once leaders are elected, the block proposal process begins. The purpose of block proposal is to provide a suggested ordering of transactions that can be accepted or rejected by the rest of the network. Each proposer (also called a leader or validator) at a given time slot assembles the most recent transactions into a block, and then shares its block with the rest of the network for approval.

Block Finalization

The final step in the process is to append a new block into the ledger, the process is called Block Finalization. The finalization procedure consists of periodically (e.g., every 50 blocks) running a voting protocol among the validators.

Security

Prevents stake grinding

The leader election is fully determined by the parent chain. In order to stake grind a hypothetical attacker would need to forecast the next block hash on the parent chain, which is highly unlikely.

Deals with forks

The Hypersign forks and the participants decide which fork to follow. When the fork on the parent chain is resolved, then it is resolved on the child - the finality of leader elections on the child chain comes with the finality of blocks on the parent chain. Hard forks are known in advance so participants of the Hypersign have plenty of time to prepare and decide which fork to support.

Long–range attack

While it is still possible to perform a long–range attack, it would be impossible to do it secretly and without preparation since the very beginning. The commitments guarantee that the information of delegates is stored in an immutable chain, and one would need to announce their will of mining suspicious blocks during the entire period of the attack. This would quickly expose the intention of the attacker and let the others prepare for a possible upcoming attack.

Use of HID coin

The Hypersign network comes with basic payment infrastructure for any party to set up a payment layer. There is no need for integrating third party payment providers or maintaining billing, managing accounts, keeping records, developing payment user interfaces, etc. All these tools come with a built into Hypersign ecosystem. Actors can pay using the HID token for services. The payment infrastructure includes;

- HID Coin - Hypersign network's native currency.
- Payment Channel - which helps to set up pay-per-usage configuration.
- Dashboard - to manage transactions.

Paying for credential

End-users can pay for credentials to the issuer directly from the identity wallet without needing to go through any Signup processes. This helps to speed up the process of issuing identities. At the time of requesting credentials, a user has to provide their DID, the signed transaction which says "user pays x HID to issuer" and user data.

An issuer can accept the payment by submitting the signed transaction in the network, verify the userdata and finally can issue the credential. This way an issuer does not have to worry about any payment related infrastructure implementation or costs to provide credential service.

Incentivizing Identity Providers

A major revenue stream for IDPs is from user-data, based on this revenue, they are able to offer free authentication and authorization services. The IDP analyzes and processes user-data to extract information and sell to advertising companies so that they can show specialised ads to the user.

The Hypersign ecosystems urge IDPs to not store user-data or even if they do store, they should store in an encrypted form which is hard to analyze and process and safe from potential hacks. However, technically it does not prevent IDPs from malpractice.

The challenge is to achieve a balance; on one hand IPDs need to be incentivized for taking care of user data and on the other hand, they need to be penalized for misusing it for processing and analyzing for the purposes which the user is not aware of. The network's token economy along with a reputation system helps to achieve both of these goals.

Technically, anyone can run a node and connect to the network to become a validator and can earn mining incentives. However, we envision IDPs to become validators of the network so that the Hypersign becomes a trusted network of reputed entities. For this we are trying to partner with many real world identity providers. There can be multiple benefits and revenue streams for IDPs who become validators;

1. Earning fees for verifying transactions and maintaining the network.
2. Earning mining rewards.2
3. Free tools like Hypersign studio, Hypersign sdk etc. for managing credentials.
4. Built-in payment infrastructure like HID coin, payment-channel, transaction explorer etc. for implementing a payment layer.
5. Earning from issuing verifiable credentials.

Incentivizing Service Providers

Service providers can also participate in the network in the form of validators and can earn mining rewards and transaction fees and other benefits as discussed in the previous section. They can also make use of all the tools available for identity and access management. This way they can issue their own credentials to their users and would not have to rely on any third party provider. Moreover, the service provider can also endorse a user with an endorsement score in the Hypersign ecosystem, which will be discussed in the next section.

User Endorsement score

Whenever a service provider authenticates or verifies a user, it can endorse the user upon successful verification. The user endorsement gets recorded in the blockchain via a smart contract. Although it is an optional feature but it helps to give more confidence about the user who is trying to access the service and will certainly help to reduce the fraudulent signups.

“The Hypersign blockchain is a hybrid network that achieves scalability by its native PoS consensus based network and security by connecting to its parent PoW network.”

Note: More details about network economy will be published in the future versions of this document.

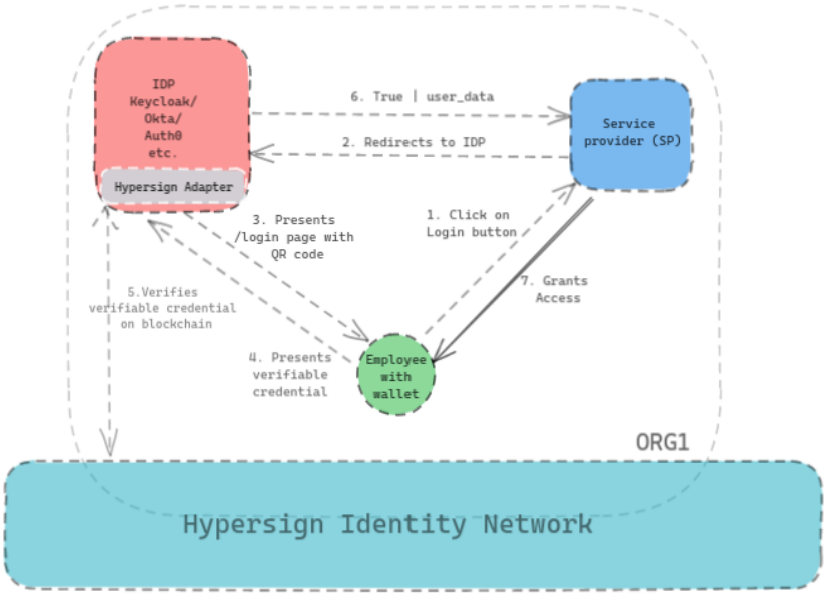
Hypersign for employees

More than passwordless

Hypersign goes one step further; not only does it eliminate the need for usernames and passwords in favor of cryptographic authentication, but it also adds the ability to exchange verifiable digital credentials for stronger, more flexible, and more resilient identity verification and access control.

Cost Effective

Participating in the Hypersign network would not just give an enterprise an opportunity to earn rewards as validators, but also get access to applications and tools for managing the identity and access control of their employees at a minimal cost. This makes it not just secure but also trust less and a very scalable solution.



Quick and easy integration with existing IAMs

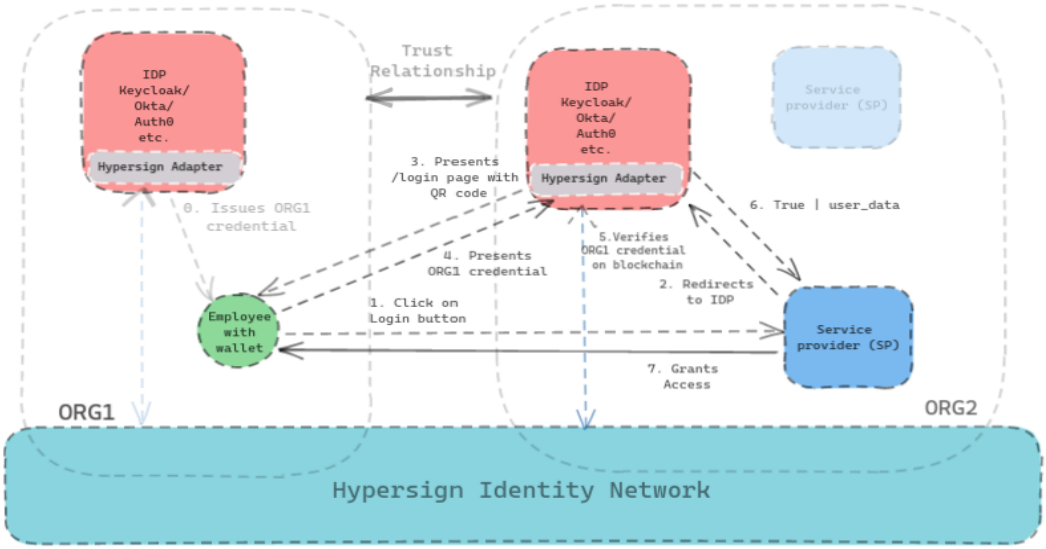
Hypersign helps enterprises to adopt passwordless authentication swiftly. Enterprises who are already using centralised IAM solutions like Okta, Keycloak or Auth0 can integrate the Hypersign Adapter to be able to provide passwordless authentication to their employees without making too much change in their existing system. Take a look at the figure above.

Federation simplified

The Hypersign simplifies the process of federation using verifiable credentials. At the initial step, a verifiable credential is issued to an employee by Org1. The Org2 supports credentials issued by Org1.

Employees use this credential to authenticate themselves to the IDP of Org2 . The Org2 verifies the credential by connecting with the Hypersign network and allows the employee of Org1 access services of Org2.

Take a look at the figure below.



"This way any enterprises get a very cost effective, integrable in minutes, scalable and decentralised IAM system which has top of the line features like passwordless authentication, Single Sign On, Federation etc."

Features & Value Propositions

Passwordless - Say No to username and passwords forever

Hypersign is built using cryptographic key-pairs and neither username nor password is required for any kind of access.

Say No to MFA

The Hypersign answers questions about all three:

- “What I know?”: The private key store in mobile wallet.
- “What I have?”: The mobile device.
- “Who am I?”: The biometric fingerprint.

There is no need to use any other factor since Hypersign answers all three questions.

Easily integrable with existing IAMs

Hypersign can easily be integrated with legacy centralised IAM systems to port them into decentralised passwordless authentication solutions.

Cost Effective

Hypersign being a decentralised system, doesn’t just bring a secure and scalable IAM system, but also helps to reduce the overall cost of IAM drastically which is well suited even for small and medium enterprises.

One click registration and login

With Hypersign, no need to fill registration forms anymore. The verifiable credentials sharing enables enterprises to quickly onboard an end user without asking them to fill any form.

Frictionless UX

No need to manually enter any credentials like username and password at the time of login. A user can login in just by scanning a QR code or just by clicking a button. Single factor mechanism of Hypersign enhances the usability even more.

Scalable

Hypersign enables service providers to verify credentials without interacting with the IDP. This helps to reduce the load from the IDP system and makes the whole system modular to scale.

Partial data sharing & Minimal Data exposure

Hypersign provides the ability to the end user to share data only what is required. Now it is possible for an end-user to share partial data with a service provider. They need not share the entire documents and fear data leakage.

Furthermore, Hypersign offers using ZeroKnowledgeProof based verification where users can share the proof of data they hold without revealing the actual data set. For example, in order to tell a service provider that a user is an adult, a user can just prove that he/she is over 18.

Control & Consent

In the Hypersign ecosystem, a user gets full control of his/her. They get the ability to hold their credentials in user-agents which only they have access to. Moreover, the end-user can decide to whom and to what extent they want to share their data and it all happens with the user consent.

Privacy by design

Hypersign infrastructure is built on the seven founding principles of Privacy by Design.

1. Proactive: Hypersign is proactive and not remedial as it anticipates and prevents privacy invasive events before they happen. It aims to prevent them from occurring.

2. Privacy - the default setting: − Hypersign provides the maximum degree of privacy by ensuring that personal data are automatically protected in any given practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy − it is built into the system, by default.

3. Privacy - Embedded : Hypersign protocol is built on cryptographic primitives such as Public Key Encryption and Zero Knowledge Proof which is embedded

into the design and architecture. It is not bolted on as an add-on. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Hypersign accommodates all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Hypersign avoids the pretence of false dichotomies, such as privacy vs. security.

5. End-to-End Security – Hypersign offers Full Lifecycle Protection. Privacy by Design having been embedded into the system prior to the first element of information being collected, extends security throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave.

6. Visibility and Transparency – Hypersign is Open and seeks to assure all stakeholders involved that it is, in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike.

7. User Centric Approach - Above all, Hypersign is designed and operates to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly ergonomics.

Hypersign Data Market & NFTs

One of the prominent use cases apart from Identity and Access Management,is to build a Marketplace for verified personal and public data that's minted in the form of NFT's.

The Self Sovereign Identity protocol proposes three stakeholder's,

a. **User** - One who holds the data
b. **Issuer** - Someone who issues credentials to the user after verifying the data
c. **Verifier** - Someone who receives verified credentials from the user

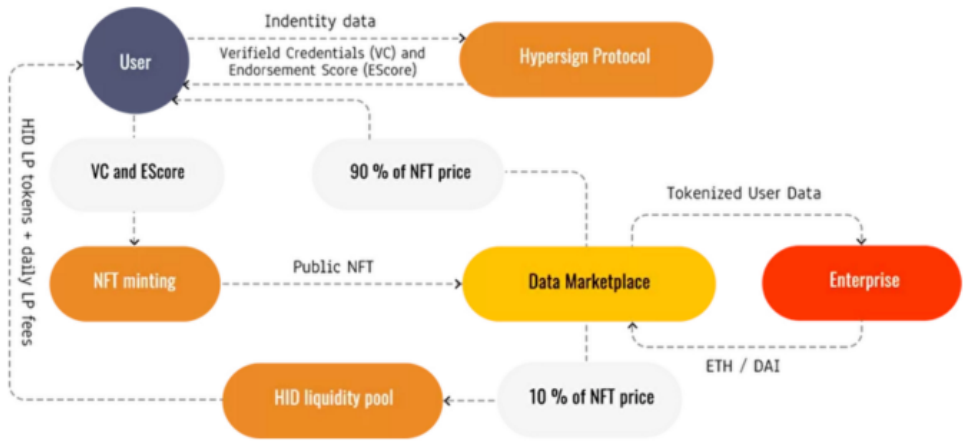
The core protocol has incentives for Issuer(Identity Providers) and Verifiers(Service Providers) in different shapes and forms, But it's very important that the User's that's the more crucial part of the ecosystem should also be incentivized.

The Marketplace

Once users receive their Verifiable Credential issued by a prominent Issuer. These verifiable credentials are privately owned by the users in their Hypersign Identity Wallet or Data Vault.

Hypersign will offer a data marketplace where users could mint NFT out of their private Verifiable Credentials. This NFT would contain some of their public information such as name and a score that defines how authentic the data is. On the other side the buyers who are looking to buy verified personal information. The buyer makes a purchase using ETH/DAI.

90% of the price is sent directly to the user and 10% goes to HID/ETH/DAI liquidity pool.
What we achieve with this is that users now can own and monetize data Investors could earn fees through HID liquidity pool.



Hypersign Product Roadmap