Talao Professional Identity Relay

Release 0.6

Read the Docs, Inc & contributors

Feb 25, 2021

Contents:

CHAPTER 1

Overview

1.1 What is Talao ?

Talao is a Blockchain protocol to manage a professional Self Sovereign Digital Identity.

Traditional architectures to validate, certify, and manage professional data are based on centralized, top-down approaches that rely on third-party private operators. Unfortunately these solutions often lead to inappropriate use of personal data and hacks. Whatever the GDPR could impose to private operators, the fact is that our data are stored on their servers and they will ultimately do what they want with our data.

Talao approaches this issue starting from a user perspective through a Blockchain Decentralized IDentity (DID) focused on professional data :

- You own your data for your lifetime.
- No one can access your encrypted data without your permission.
- No storage costs.
- Claims are verifiables, tamper proof and trackable.
- Claims issuers are identified.

Talao allows Professional Identities for Talents, Companies and claims issuers such as Schools or Training Centers. It is for everyone the opportunity to use a new technology to get tamper proof professional data while keeping the ownership of those data.

Identities with their verifiable claims can be displayed anywhere on digital platforms : social medias, websites, Job boards, etc. They provide to third parties reliable data about professional experiences, skills and education.

Terminology : in this document we will consider "Self Sovereign Identity" as an equivalent to 'Decentralized IDentity'.

1.2 How does Talao work ?

Talao is based on Ethereum smart contracts Identities.

Smart contract Identities are like digital vault where you can store your data as Digital ID, diplomas, professional certificates, business contracts, pay slips,... Each individual or company is given its own private key to access and update its Identity.

Thanks to cryptographic algorithms those private keys are only used to sign messages sent by the Identity owner to the Blockchain servers. If someone wants to update its data, he/she will sign a message with a private key and send it to all Blockchain servers. Each server will check the signature, update data then compare them to other server copies. As those data are duplicated on thousands of servers, no one can alone hack the Identity.

This Talao web application https://talao.co is a trust service to access Self Sovereign Identities with a simple User Interface and automated processus. From a blockchain perspective, the Identity owner is the Ethereum account attached to the the smarthone crypto wallet.

1.3 What are Decentralized IDentities (DID) ?

The Decentralized Digital Identity concept is based on the use of Decentralised Identifiers. As defined in the current DID specification of W3C1 :

"Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document may contain at least three things: proof purposes, verification methods, and service endpoints. Proof purposes are combined with verification methods to provide mechanisms for proving things. For example, a DID Document can specify that a particular verification method, such as a cryptographic public key or pseudonymous biometric protocol, can be used to verify a proof that was created for the purpose of authentication. Service endpoints enable trusted interactions with the DID controller."

Furthermore eIDAS regulations now in place in Europe are taking the opportunity to include Self Sovereign Identiy technologies to expand security and data protection (see the SSI-eIDAS Bridge project launched by EU)..

More information available :

- https://identity.foundation/
- https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf
- https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about

1.4 What blockchain support does Talao use ?

Talao is available on the public Ethereum Mainet and Rinkeby. See https://github.com/TalaoDAO/talao-contracts for details.

Talao is also available on a private Ethereum network named TalaoNet. TalaoNet runs a Proof Of Authority consensus (Clique) managed by the Talao team and partners.

To connect to this blockchain use RPC URL https://talao.co/rpc

Main contract addresses are :

- Talao token : 0x6F4148395c94a455dc224A56A6623dEC2395b99B
- Foundation : 0xb4C784Bda6A994f9879b791Ee2A243Aa47fDabb6
- Workspace Factory : 0x0969E4E66f47D543a9Debb7b0B1F2928f1F50AAf

1.5 Credits

Thanks to the Ethereum community which provide us with great tools, Solidity code and inspiration.

Special thanks to the WalletConnect team for their implementation of an awesome protocol to connect crypto wallets with Dapps.

Special thanks to OriginProtocol for their implementation of ERC 725 and ERC 735, which we use with slight modifications.

Thanks to the NLTK team and community for their Natural Language Programming work we used in the Dashboard panel is based on the python librairy NLTK. For more information Bird, Steven, Edward Loper and Ewan Klein (2009), Natural Language Processing with Python. O'Reilly Media Inc.

CHAPTER 2

Privacy

2.1 Overview about encryption and privacy

An Identity is a smart contract on the public Ethereum Blockchain or a private Blockchain (POA). Identity is defined by its own Ethereum address. This smart contract is created at setup by his owner (person or company) through the owner Ethereum address and his associated private key.

In order to get strong privacy, the Talao protocol uses 3 specific AES encryptions keys (one for public data, one for private data, one for secret data) to encrypt user data. 2 keys (private and secret) are stored within the Identity encrypted with a RSA key, the third one for public data is available within the open code. User data are mainly stored on a decentralized file system IPFS.

Consequently for Individuals there are several ways of using the web platform depending of who can access to the owner Ethereum private key and his encryption keys :

- If the Identity has been setup by the website https://talao.co, the website server is a **third party wallet**, it has a copy of the Ethereum Private key and RSA key. They are stored on a Centralized server. We say that the Identity is **managed on behalf of the identity owner**. All services are available through the website which is a classic web application.
- If the Identity has been setup externally by a user (see freepdapp), the website is **fully or partially activated** to act as an agent and sign transactions on behalf of the owner. In this case the server does not have a copy of the Ethereum private and RSA keys but the user has limited access to the website services. For instance certificate issuance and Partnership services are not available.
- An other solution is to setup an identity through the website then later do a **Change of ownership** : Identity is setup by the website and later on the Identity is transfered to an Ethereum address setup secretly by the owner. In this case the server does not have a copy of the Ethereum private key. This solution has the advantage to be easy and fast. Certificate issuance services will not be available but the identity will able to receive certificates from others.

Note: For users who mainly want to request certificates, the easiest solution is to get an Identity **managed on behalf of the owner** by Talao.

List of website services :

- Edit personal settings,
- Edit resume (Experience, Education, . . .)
- Issue certificates,
- Reqest certificates,
- Manage Partnership,
- Manage Alias,
- Manage Referent,
- Manage White List,
- Invit user,
- Store files.

2.2 Two-factors authentification

If they do not have their smartphone one hand, user can acces their Identity with their username and paswword. In this case they have a limited access to their Identity but they can build their resume. For security we uses a two-factors authentification protocol for this type of authentication.

Wikipedia : "Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is). Two-factor authentication (also known as 2FA) is a type, or subset, of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are."

Dynamic passwords (named secret code) are random numbers that are used once to authenticate. Every time an end user wants to login, he enters his usual static password and a secret code sent in real time by Email or by short messages on the user's Phone. The secret code lifetime is 3 minutes.

Dynamic passwords are convenient because they don't have to be remembered, and because the password is never the same, they serve as a major roadblock for hackers who may be looking to break into user accounts.

Note: By default at setup the static password is 'identity' and scret code are sent by email. Once logged, one can change the static password and choose sms to receive your secret code on your phone.

2.3 Data and privacy

Data are either public, private or secret data

Private and Secret data are protected by AES encrypted keys which are themselves stored encrypted on Ethereum with an RSA key. Public data are encrypted with an AES key stored within the code.

Warning: The private and secret keys are determined at Identity creation and cannot be changed later on.

At creation users can decide what level of privacy for :

- Personal data (except for firstname and lastname which are always required and public)
- File (Data store).

Experiences, Certificates and Education are always Public data.

Public Data is available for anybody :

- For Talents, by default Firstname and Lastname are Public.
- For Companies, by default all profil data are Public.

Private Data are only available for your Partners. Read more on *Professional Identity* .

Secret Data are only available for users.

- Users can store encypted data on decentralized support as IPFS through this option.
- Authentification Email is always secret (Relay keeps a copy of ths email for authentification)
- By default for Talents, Email and phone are secret, used for authentification only.

CHAPTER 3

Professional Identity

A professional Decentralized Identity is made up of data relating to individuals career, skills and experience.

3.1 Personal settings

They are traditional information one can get in a resume :

- Firstname, lastname, contact email, contact phone, bithdate, about, postal address

Warning: By default those personal data are given by user through the Relay which is an automatic 'Issuer'.

They are eventually not reliable for third parties as data are either self declared or issued on user behalf.

3.2 Proof of Identity

This is one of the most important feature of the Identity.

In order to get reliable data, one has to prove the user belonging of the Identiy and the liability of personal data.

This process is today manage only by Talao through a KYC process for Talents and Companies. Read more on *Get a Proof of Identity*

Note: We strongly suggest to ask Talao for a Proof of Identity as soon as possible. They are currently free of charge

3.3 Experience

Experience data are always Public. Those Experiences are issued by yourself. They are an essential part of a standard resume. Those data are self declared.

3.4 Education

Education data are always Public. Those Educations are issued by yourself only. They are an essential part of a strandard resume. Those data are self declared.

3.5 Certificates

Certificates are always public.

They have a strong added value as they are issued (signed) by third parties and so data can be checked for reliability and proof of issuance.

There are several types of certificates :

- Experience Certificates issued by companies
- Skills and Trainng Certificates issues by companies (Not implemented yet in July 2020)
- Recommendation issued by Companies or Persons

One can check the issuer of each of those certificates. For each issuer one can check its proof of identity and its own certificates. This process can be done as long as one find strong proofs of evidence.

One can make a copy of the certificate link to insert them anywhere in digital presentation. Certificate links can be deleted by user from his/her Identity. However if the link is deleted the certificate is always "live" on its decentralized support as data are tamper proof.

3.6 Alias

An Alias is a new couple of Username+Email for authentification through the Relay

At setup, one smart contract is created for each identity and one authentification email is encrypted and stored within this smart contract on the Ethereum Blockchain. The address of the smart contract is the Decentralized IDentifier (DID) of the Identity. Unfortunaltly theis address is quite difficult to memorize (ex : 0xfC6acd13F07bcCFB7563908f717377806e0Ed92E). So when user signs in the first time, he registers a "username" to have a readable identifier associated to his smart contract address.

An Alias is another Username you can use with another email to access yous Identity through the Relay.

You can add as many Alias you want, for instance you can use an Alias for each of your device.

3.7 Referent

A Referent is a Company or a Person the user has authorized to issue certificates. The user is the only one able to appoint Referents. User does not need the Referent authoriation to appoint him/her. In the other hand the Referent is not obliged to issue any certificate to the user.

3.8 Partner

A Partner is a Company or a Person with whom you share Private data.

A partnership is the relationship you share with your Partner. You can request a partnership but it has to be accepted by other party to be effective.

Any party can cancel a partnership at anytime.

Warning: When a partnership is established you share your private data. After cancellation the other party can eventualky keep on using your private key to access your private data.

3.9 White List

The White List is made up of reliable issuers from your standpoint. You can add a new issuer in your White List through the White List menu. It is likely your own Referent and Partners are reliable but you have to add them anyway, you can also add other Issuers even if they are not in your Referent List.

This White List allowed you to have better view of others certificates.

Note: By default Relay is not a White List issuer, but Talao is. At start Talao is the only company to issue Proof of Identity.

3.10 Data Store

The Data Store is decentralized support to store data you either want to share with others (public privacy) or only with Partners (private privacy) or you want to keep secret for everybody.

If you want to change the nature of the privacy you firtst need to remove the file and create a new one. The document will be encrypted at creation and stored on a decentralized support (IPFS today).

3.11 Advanced

This information is usefull to check and track your data through other means as Ethereum Explorer

Relay Status : Activated if user has given to the Relay the right to sign on behalf the Identity. If Relaus does not have this right, no data can be updated through the Relay application.

Private Key : Yes or No. If True the Relay has a copy of the Ethereum private key og the Identity. This is the case when the Identity is created through the Relay (Quick Start).

RSA Key : Yes or No. If No Relay cannot crate Private or Secret data.

CHAPTER 4

Quick Start

You can access your Digital Identity through your desktop or smartphone.

Note: For registration you need your desktop and your smartphone.

4.1 Register

- if you do not have a crypto wallet on your smartphone, download one and setup your account. Best is to use Metamask for mobile (IOS, Android). A list of the other wallets available are here (more than 50). Currently we are using for testing purpose : Trust https://trustwallet.com/, Rainbow https://rainbow.me/, TokenIm https://token.im/" and Matic https://matic.network/wallet/.
- go to https://talao.co with your desktop viewer and clic on "Connect with wallet",
- open your crypto wallet, look for the walletconnect tool scan and scan the QR Code displayed on your desktop screen.
- follow the process. A new Identity will be proposed if you do not have one.
- Enter firstname, lastname, email and phone number for authentification purpose.

Note: Your crypto wallet will be used only for authentification purpose. This process is safe for your wallet and free (no transaction). Your wallet account wont be displayed to public. Your private key remains in your smartphone wallet. Talao has no access to your wallet.

The process to create an Identity will take a couple of minutes depending of the load of the Network. Authentification is made by message signing (no costs).

4.2 Login

For login you can use either your smartphone viewer alone or your desktop viewer and smartphone.

- Go to https://talao.co and scan the QR Code with your smartphone wallet scan tool.
- Complete your profil as much as possible and request certificates to Companies or Individuals. Read more in *Request a Certificate*

4.3 Support

If you are having issues, please let us know. We have a mailing list located at: relay@talao.io

CHAPTER 5

Request a Certificate

If you are new and you do not have an Identity, it takes about 5 minutes :

- First, create your own Identity. Go to https://talao.co/register/ and enter your firstname, lastname and an email for authentification.
- When you receive your username and private keys go to https://talao.co to log and acces your Identity
- Then clic on "Request Certificate" of the Menu Bar and follow the process.

Note: To request a Certificate, you will need to know your referent's email. He/Her will receive an email with a link to setup your certificate. In order to have reliable data, the referent will also setup his/her own Identity during the process.

5.1 Types of Certificates

So far there are 2 types of Certificates available :

- Experience Certificates
- Recommendations (Person to Person)

More to come :

- Skill Certificate,
- Training Course and Education Certificates

5.2 Experience Certificates

Fill the form to issue the Certificate as precisely as possible. It will be used by the Issuer to draft your Certificate.

Do not forget to write a memo to your Issuer. This memo wil be added as the first lines of the email.

The issuer will answer to 4 questions with an evaluation from 1 to 5 stars :

- How satisfied are you with the overall delivery ?
- How likely are you to recommend this talent to others ?
- How would you rate his/her ability to deliver to schedule ?
- How would you rate his/her overall communication skills ?

All the data of this Certificate will be tamper proof. The certificate will be visible through a link to your Identity. You can copy this link to your social media or send it to your future employeer or you can delete it.

In order to strengthen your Certificate best is to get a Proof of the Identity.

5.3 Recommendations

It is a basic referral from person to person (free form text area).

The recommendation will be visible through a link to your Identity. You can copy this link to your social media or send it to your future employeer or you can delete it.

CHAPTER 6

Get Rewards (in progress)

You can get rewards in TALO tokens depending of your involvment. To receive Rewards you muts have a

- Proof of Identity issued by Talao, see how to obtain this document on *Get a Proof of Identity*,
- a registered phone nUmber for authentification purpose

Tokens will be automatically transfered to your Identity Address after

- Invitation : 10 TALAO tokens after confirmation of subscription of a new Indentity with Proof of Identity
- Issue a Certificate : 10 TALAO tokens

CHAPTER 7

Add a Referent

A Referent is a Company or a Person the user has authorized to issue certificates. The user is the only one able to appoint Referents. User does not need the Referent authorization to appoint him/her. In the other hand the Referent is not obliged to issue any certificates to the user.

To appoint a Referent, there are 2 options :

- the Referent has an Indentity and you know his/her username. In this case you just have to search the Referent with the Search Bar and Clic on the Service option.
- the Referent does not have any Identity. You must first invite him.

CHAPTER 8

Use my own Ethereum Address

Managing your Professional Identity through your own Ethereum Address gives you the possibility to keep the entire ownership of your data and receive certificates while using an easy website service to acces your Identity. However the limitations are :

- you will not be able sign certificates for others,

The process to setup your Identity takes about 15 minutes and you need to master the signature of transactions on Ethereum through your wallet.

If you want to use your own Ethereum Address to mamage your Professional Identity, follow the steps :

- Step 1, you need to get 100 TALAO tokens and transfer them to your Ethereum Address. You can get them on IDEX https://idex.market/eth/talao. If you cannot buy them there, contat us at relay-support@talao.io.
- Step 2, you need to open an access to the Talao Protocol. This can be done through the TALAO token : go to https://etherscan.io/token/0x1d4ccc31dab6ea20f461d329a0562c1c58412515. Select "Write Contract" in the menu, connect with web3 through your Ethereum Address (wallet Metamask, or other) to be able to send a transaction to the contract. Look for createVaultAccess function (#11), fill the field with with value 0 and confirm the transaction. The transaction will lock 99.99 TALAO tokens from your Ethereum Address.
- Step 3, go to http://talao.co:5000/use_my_own_address/ and follow the process to create your Professional Identity with your own Ethereum Address.

Note: Do not use the same Ethereum Address as the one you use to buy crypto funds. Setup a specific Ethereum Address for your Professional Identity.

Warning: JULY/AUGUST 2020 TESTS. We currently are using Rinkeby testnet. DO NOT USE ETHEREUM TOKEN but Rinkeby Token. Contact us to get your 100 TALAO tokens at relay-support@talao.io

To open an access to the Talao protocol go to https://rinkeby.etherscan.io/address/0xb8a0a9ee2e780281637bd93c13076cc5e342c9ae choose "Contract" in the menu then "Write Contract".

CHAPTER 9

Get a Proof of Identity

So far Proof of Identity are only delivered by Talao.

For individuals we need 2 pictures

- your Identity Card or Passport
- a selfie with your Identity Card or Passport in hand.

On both pictures we must see your face and Identy Card Picture and all information must be readable. We will issue a Proof of Identity within 48 hours or will send you an email if we cannot check the data.

For companies send an email through your authentification email to contact@talao.io.

CHAPTER 10

Sign documents and emails with your Identity

So far digital signature are managed by International standards of cryptography as X509.

[wikipedia] "... In cryptography, X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS,the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key."

In order to allow user to sign documents and emails with his/her decentralized Identity, Talao provides X509 certificates attached to Identity. Those certificates are signed by Talao as a Certification Authority. You will get two certificates as files xxxx.p12 and xxxx.pem. Thoses cestificates will be needed to sign and encrypt data with your email client.

Sign in, chose your Identity page, clic on "Advanced" in the top right menu and then clic on "RSA key and x509 Certificates".

To install those certificates in SMTP clients :

For Thunderbird Mozilla : https://www.ssl.com/how-to/installing-an-s-mime-certificate-and-sending-secure-email-in-mozilla-thunderb

For Outlook : https://www.thesslstore.com/knowledgebase/email-signing-support/install-e-mail-signing-certificates-outlook/

To sign documents (PDF, image, ...)

https://getoutpdf.com/sign-pdf-with-certificate-x509

CHAPTER 11

Talao Connect API

The Talao API server is an OpenID Provider for decentralized self-sovereign Identity.

Talao Connect APIs can be used for authentication, identification, claims issuance and more generally for Identity management. For instance in the Human Resource sector it is an easy way to get reliable data about Talents and a powerfull and secure tool for onbarding user while keeping their data safe.

Those API do not provide basic account setup (details, signature, logo ...) which are available through the web platform https://talao.co .

Standard use cases for APIs are :

- Issue claims (certificates, diplomas, agreements, ...) to persons, companies and all sorts of organizations.
- Authenticate users who have their own Decentralized Identity.
- Create decentralized Identities for others.
- Strenghen an employer brand with latest technology features like Blockchain Resume, Decentralized Identity,...

We use OpenID Connect Autorization Code flow for authentification and OAuth 2.0 Authorization code flow and Client Credentials flow to manage user access to their identity.

Contact us relay-support@talao.io to open your Company Identity and receive your application granted permissions to use those APIs.

From the OIDC and OAuth 2.0 perspective :

- "Company" is the Client application
- "User" is the Resource Owner, it maybe a Talent or another Company
- "Talao API server" is the Authorization Server/Resource Server

11.1 Resolver

The Resolver allows to get public data about and Identity. It provides for a username or a DID (Decentralized IDientifier) the asssociated DID or username, the Identity owner address and the RSA Public Key to authenticate the

Identity.

```
curl  -H "Content-Type: application/json" -X POST https://talao.co/resolver/  -d '{
↪"input" : "thierrythevenet"}'
```

Return is a JSON structure :

Resolver has a standard UI access at http://talao.co/resolver

CHAPTER 12

OpenID Connect

For your users (as a person), the OpenID Connect authentication experience includes a consent screen that describes through 'scopes' the information that the user is releasing. For example, when the user logs in, they might be asked to give your appication access to their name, email address and basic account information. You request access to this information using the scope parameter, which your app includes in its authentication request.

12.1 Scopes available

Scopes for data access are standard OpenID Connect and specific Talao scopes :

- openid (required to get a JWT)
- profile (sub + given_name + family_name + gender)
- birthdate
- email
- phone
- address
- about : short user description
- resume (in progress on 11-17-2020) : for person identity only
- proof_of_identity (in progress on 11-17-2020)

Note: "sub" is the Decentralized IDentier of the user (did). It always starts with "did:talao:".

Those data are available through an ID Token (JWT) and at the user_info endpoint with an Access Token.

For companies, there is only the "openid" scope available.

12.2 Process

As defined by OIDC, 3 steps are required :

Step 1 : to get a grant code from user, redirect your user to https://talao.co/api/v1/authorize with a subset of your scope list . User will be asked to sign in with his Identity username/password and to consent for your list of scopes. scope "openid" is required to get a JWT.

Example :

```
https://talao.co/api/v1/authorize?response_type=code&client_id=your_client_id&
↪scope=openid+profile&state=state&nonce=nonce
```

Step 2, with the grant code, connect to the token endpoint https://talao.co/api/v1/auth/token to get an Access Token and an ID Token. You will need your client_secret.

```
curl -u your_client_id:your_secret_value -XPOST https://talao.co/api/v1/oauth/token -
↪F grant_type=authorization_code
```

If you only need user authentication, see further how to decode the JWT and get user data with server signature.

Step 3 : with the Access Token you can also get user data through the user_info endpoint https://talao.co/api/v1/user_info.

```
curl -H "Authorization: Bearer your_access_token" https://talao.co/api/v1/user_info
```

Return is JSON (example) :

```
{
  "sub": "did:talao:talaonet:81d8800eDC8f309ccb21472d429e039E0d9C79bB",
  "given_name": "Thierry",
  "family_name": "Thevenet",
  "gender": null,
  "email": "thierry.thevenet@talao.io",
  "phone": null,
  "resume": {}
}
```

12.3 Decode JWT

JWT can be decoded with Talao RSA public key . Audience is 'did:talao:talaonet:EE09654eEdaA79429F8D216fa51a129db0f72250', algorithm is RS256

Talao RSA key :

```
-----BEGIN PUBLIC KEY-----
↪\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3fMFBmz2y31GlatcZ/
↪ud\nOL9CmCmvtde2Pu5ZggILlBD6yll+O10eH/
↪8J8wX9OZG+e5vAgT5gkzo247ow4auj\niOA87V9bdexI7nUiD5qjdKTcIofJiDkmCIgF/
↪UqwQ7dfyl1jWDVB1CnfAqkL0U2j\nbU+Nb/y1M1/
↪oTFoid+trRFbhM+0awr06grh4viGJ0i5oVCcuybcDuP7bwNiZD1FP\n85L/
↪hlfXvJs+oz6K+583leu1hj7wFnWSv0jgeYHkdgoG3rSKlbTxt+98dTu3Hy8s\nePl9O/
↪2WKi6SSH0wpR+FqaBULAAyWd0cj5mjBLYoUiGP7qyIU5/9Z+pVf+L7SO7t\nlQIDAQAB\n-----END␣
↪PUBLIC KEY-----
```

JWT payload example :

```
{
"iss": "did:talao:talaonet:EE09654eEdaA79429F8D216fa51a129db0f72250",
"aud": ["did:talao:talaonet:EE09654eEdaA79429F8D216fa51a129db0f72250"],
"iat": 1603895896,
"exp": 1603899496,
"auth_time": 1603895896,
"nonce": "64867",
"at_hash": "uAaDX0YA4NnMkO6fW8-7nw",
"sub": "did:talao:talaonet:81d8800eDC8f309ccb21472d429e039E0d9C79bB",
"given_name": "Thierry",
"family_name": "Thevenet",
"gender": null,
"email": "thierry.thevenet@talao.io",
}
```

CHAPTER 13

OAuth 2.0 Authorization code flow

For your users, this flow includes a consent screen that describes through 'scopes' the actions that the user allows to your application. For example, when the user logs in, they might be asked to accept or reject a partnership.

There is no off-line access through Refresh Token but Talao partnership allows your company to get user data as long as the partnership is authorized. However it means that you always need consent of an online user who signed-in Talao to issue or delete a certificate on his/her behalf.

Note: If your company needs to sign a certificate as an issuer, see further the Client Credential flow.

You request an access to these functionalities using the scope parameter, which your app includes in its request.

Below list of scopes :

- user:manage:certificate : This scope if accepted by user allows your company to issue/delete certificates on behalf of a user
- user:manage:partner : This scope if accepted by user allows your company to request, accept or reject partnerships with all Identities on behalf of a user
- user:manage:referent : this scope if accepted by user allows your company to add or remove referents on behalf of a user
- user:manage:data : this scope if accepted by user allows your company to add or remove data (account settings) on behalf of a user

Step 1, ask for a grant code with your scope list, nonce, state.

```
https://talao.co/api/v1/authorize?response_type=code&client_id=your_client_id&
↪scope=your_scopes&state=state&nonce=nonce
```

Step 2, with the grant code, connect to the token endpoint https://talao.co/api/v1/auth/token to get an Access Token. You will need your client_secret.

```
curl -u your_client_id:your_secret_value -XPOST https://talao.co/api/v1/oauth/token -
↪F grant_type=authorization_code
```

Access Token is live 500 seconds.

Step 3, with the Access Token you can acces an endpoint

```
curl -H "Authorization: Bearer your_access_token" -H "Content-Type: application/json"␣
↪ https://talao.co/api/v1/endpoint  -d your_json_data
```

13.1 Endpoint : POST https://talao.co/api/v1/user_issues_certificate

Issue a certificate to an Identity(person or company) on behalf of a user. certificate is “reference” or “agreement or “experience” or “skill” or “recommendation”. User must be in the identity’s referent list.

Scope required : user:manage:certificate

Issue an agreement certificate :

```
$ curl -X POST https://talao.co/api/v1/user_issues_certificate  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"did_issued_to" : "did:talao:talonet:2165165", "certificate_type" : "agreement",
↪ "certificate": agreement_JSON_certificate}'
```

Example of a agreement_JSON_certificate :

```
{
  "registration_number" : "2020-11-31003",
  "title" : "IQ - ISO9001:2020",
  "description" : "Quality Management Process",
  "standard" : "ISO 9001",
  "date_of_issue" : "2020-11-01",
  "valid_until" : "2030-10-31",
  "location" : "Toulouse Bordeaux Paris",
  "service_product_group" : "Drone Serie production line",
}
```

Issue a reference certificate :

```
$ curl -X POST https://talao.co/api/v1/user_issues_certificate  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"did_issued_to" : "did:talao:talonet:2165165", "certificate_type" : "reference",
↪ "certificate": reference_JSON_certificate}'
```

Example of a reference_JSON_certificate :

```
{
  "project_title" : "Ligne de production moteur NFG-1000",
  "project_description" : "Conception, réalisation et installation d'une nouvelle␣
↪ligne de production",
  "project_budget" : "2000000",
  "project_staff" : "12",
  "project_location" : "Bordeaux",
  "start_date" : "2019-02-22",
  "end_date" : "2020-01-25",
  "competencies" : ["CATIA V6",],
  "score_recommendation" : 4,
```

(continues on next page)

(continued from previous page)

```
  "score_delivery" : 3,
  "score_schedule" : 4,
  "score_communication" : 4,
  "score_budget" : 4,
 }
```

13.2 Endpoint : POST https://talao.co/api/v1/user_accepts_company_partnershi

This is a straightforward process to build a partnership with an Identity. It combines your company request for a partnership and an authorization from Identity.

Scope required : user:manage:partner

```
$ curl -X POST https://talao.co/api/v1/user_accepts_company_partnership  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
```

JSON return :

```
{
 "partnernship_in_identity": "Authorized",
 "partnership_in_partner_identity": "Authorized",
}
```

13.3 Endpoint : POST https://talao.co/api/v1/user_updates_company_settings

To update identity settings of a company. You can set 'name','contact_name','contact_email','contact_phone','website', 'about', 'staff', 'mother_company', 'sales', 'siren', 'postal_address'. If no data is provided you get all current Identity settings.

Scope required : user:manage:data

```
$ curl -X POST https://talao.co/api/v1/user_updates_company_settings  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -d '{"staff" : "6"}'
```

JSON return :

```
{
  "name" : "Talao",
  "contact_name" : "Nicolas Muller",
  "contact_email" : "nicolas.muller@talao.io",
  "contact_phone" : "0607182594",
  "website" : "https://talao.co",
  "about" : "Talao focuses on professional identity management based on an extension␣
↪of the ERC725 protocol, through a BtoB go-to-market strategy and a network of␣
↪partners to develop compatibility with corporate IT systems.",
  "staff" : "6",
  "sales" : "3200000",
  "mother_company" : null,
  "siren" : "837674480",
  "postal_address" : null
}
```

13.4 Endpoint : POST https://talao.co/api/v1/user_uploads_signature

To add a signature file to an Identity. Image format are jpeg, png, jpg. Image will be displayed with size in pixels : height=”150” width=”200”.

Scope required : user:manage:data

the Content-Type of the Header of the POST request will be multipart/form-data.

```
$ curl -X POST https://talao.co/api/v1/user_accepts_company_referent  \
-H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9"  \
-H "Content-Type : multipart/form-data" \
-F "data=@signature.png"
```

JSON return :

```
{
 "hash": "QmNr71LjJPGUYKASinx2R5u63Zpmj8ZUqniFxHhqqHBujh"
}
```

13.5 Endpoint : POST https://talao.co/api/v1/user_uploads_logo

Same as prevous one with logo. Image will be displayed with size in pixels : height=”200” width=”200”.

13.6 Endpoint : POST https://talao.co/api/v1/user_accepts_company_referent

To add your company in the Identity referent list

Scope required : user:manage:referent

```
$ curl -X POST https://talao.co/api/v1/user_accepts_company_referent  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9"
```

JSON return :

```
{
 "referent": true
}
```

13.7 Endpoint : POST https://talao.co/api/v1/user_adds_referent

To add an Identity to the user referent list

Scope required : user:manage:referent

```
$ curl -X POST https://talao.co/api/v1/user_adds_referent  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"did_referent" : "did:talao:talaonet:fA38BeA7A9b1946B645C16A99FB0eD07D168662b"}'
```

JSON return :

```
{
 "referent": true
}
```

CHAPTER 14

OAuth 2.0 Client Credentials Flow

This flow allows your company to access functionalities previously authorized by users (as referent and/or partner) and to manage your own company identity.

To create Identities :

- https://talao.co/api/v1/create_person_identity : to create an identity for a person (with partnership setup)
- https://talao.co/api/v1/create_company_identity : to create an identity for a company (with parnership setup)

As a partner of an Identity

- https://talao.co/api/v1/get_certificate_list : to get the list of all certificates of an Identity
- https://talao.co/api/v1/get_certificate : to get certificate data

To manage your own Identity

- https://talao.co/api/v1/issue_experience : to issue experience certificates to a person after your company has been appointed as a referent
- https://talao.co/api/v1/issue_skill : to issue skill certificates to a person after your company has been appointed as a referent
- https://talao.co/api/v1/issue_recommendation : to issue recommendation certificates to a person after your company has been appointed as a referent
- https://talao.co/api/v1/issue_agreement : to issue agreement certificates to a company after your own company has been appointed as a referent
- https://talao.co/api/v1/issue_reference : to issue reference certificates to a person after your company has been appointed as a referent
- https://talao.co/api/v1/get_status : to get your own referent/partner status with an identity

Using the Client Credentials Flow is straightforward - simply issue an HTTP GET against the token endpoint with both your client_id and client_secret set appropriately to get the Access Token :

Scope are required for most endpoints.

```
$ curl -u your_client_id:your_secret_value -XPOST https://talao.co/api/v1/oauth/token␣
↪-F grant_type=client_credentials -F scope=your_scope
```

To call an endpoint :

```
$ curl -H "Authorization: Bearer your_access_token" -H "Content-Type: application/json
↪" https://talao.co/api/v1/endpoint   your_json_data
```

Your Access Token will be live for 3000 seconds.

14.1 Endpoint : POST https://talao.co/api/v1/issue_experience

Issue an experience certificate to a user. Company must be a in the user's referent list.

Scope required client:issue:experience.

Issue an experience certificate :

```
$ curl -X POST https://talao.co/api/v1/issue_experience  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"did" : "did:talao:talonet:2165165", "certificate": JSON_certificate}'
```

Example of a JSON_certificate :

```
{
  "title" : "Chef de projet Blockchain",
  "description" : "Conception et realisation d un prototype Ethereum d un suivi de␣
↪production",
  "start_date" : "2018/02/22",
  "end_date" : "2019/01/25",
  "skills" : ["Ethereum", "Solidity"],
  "score_recommendation" : 2,
  "score_delivery" : 3,
  "score_schedule" : 4,
  "score_communication" : 4,
}
```

JSON return :

```
{
  "link": "https://talao.co/certificate/?certificate_
↪id=did:talao:talaonet:81d8800eDC8f309ccb21472d429e039E0d9C79bB:document:12",
  "type" : "experience",
  "title" : "Chef de projet Blockchain",
  "description" : "Conception et ralisation d un prototype Ethereum d un suivi de␣
↪production",
  "start_date" : "2018-02-22",
  "end_date" : "2019-01-25",
  "skills" : ["Ethereum", "Solidity"],
  "score_recommendation" : 2,
  "score_delivery" : 3,
  "score_schedule" : 4,
  "score_communication" : 4,
  "manager" : "Director",
  "reviewer" : "",
```

(continues on next page)

(continued from previous page)

```
  "logo" : "QmRgLUZbLfRR7hW4CB7tqTFrjrfXxVUaP3XnNjC5D5QzT",
  "signature" : "QmHT7UZbLfRR7hW4CB7tqTFrjrfXxVUaP3XnNjC5D5Qzza",
  "ipfs_hash" : "QmH456ab656446564f",
  "transaction_hash" : "46516871335453AB354654CF551651"
}
```

14.2 Endpoint : POST https://talao.co/api/v1/create_person_identity

Create an Identity for a user. Your company is appointed as a referent to issue certificates to this user. Your company is apointed as a partner to access all data without any new user authorization. User Identity username/password are sent by email to user by defaul. Setup "send_email" to False to disable. Return JSON with did (sub) and username.

Scope required : client:create:identity

> **Warning:** As your company has an access to all user data, you should give users access to their identity in order them to manage authorizations by themselves.

Create a new person identity :

```
$ curl -X POST https://talao.co/api/v1/create_person_identity \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"firstname":"jean", "lastname":"pascalet", "email":"jean.pascalet@talao.io",
↪"send_email" : false}'
```

JSON Response

```
{
  "did": "did:talao:talaonet:b8a0a9eE2E780281637bd93C13076cc5E342c9aE",
  "username" : "jeanpascalet",
}
```

14.3 Endpoint : POST https://talao.co/api/v1/get_status

Get the referent and partnership status of a user with your company.

No scope required.

```
$ curl -X POST https://talao.co/api/v1/get_status  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"did" : "did:talao:talaonet:fA38BeA7A9b1946B645C16A99FB0eD07D168662b"}'
```

JSON return :

```
{
 "partnernship_in_identity": "Pending",
 "partnership_in_partner_identity": "Authorized",
 "referent": false
}
```

partnership_in_identity :

- Authorized : your company has requested a partnership or accepted the partnership.
- Pending : user is waiting for your decision to accept or reject his request for partnership.
- Removed : your company removed the partnership.
- Unknown : no partnership.
- Rejected : your company refused the user request for partnership.

partnership_in_partner_identity :

- Authorized : user has requested a partnership or accepted your request.
- Pending : user has received your request for partnership but still pending.
- Rejected : user refused your request.
- Removed : user removed the partnership.
- Unknown : no partnership.

referent :

- False/True : is your company in the user's referent list.

Note: A partnership is effective when both partnership_in_partner_identity and partnership_in_identity are "Authorized".

14.4 Endpoint : POST https://talao.co/api/v1/create_company_identity

Create an Identity for a company.

Your company is appointed as a referent to issue certificates to this company. Your company is apointed as a partner to access all data without any new user authorization. User Identity username/password are sent by email to user by default, Setup "send_email" to False to disable. Return JSON with did (sub) and username.

Scope required : client:create:identity

> **Warning:** As your company has an access to all user data, you should give users access to their identity in order them to manage authorizations by themselves.

Create a new identity :

```
$ curl -X POST https://talao.co/api/v1/create_company_identity \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"name":"NewIndus", "email":"jean.petit@newindus.io", "send_email" : false}'
```

JSON Response

```
{
  "did": "did:talao:talaonet:1a50a9eE2E780281637bd93C13076cc5E342c9aE",
  "username" : "newindus",
}
```

14.5 Endpoint : POST https://talao.co/api/v1/issue_reference

Issue a reference certificate to a company. Your company must be a in the company's referent list.

Scope required client:issue:reference

Issue a reference certificate :

```
$ curl -X POST https://talao.co/api/v1/issue_reference  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"did" : "did:talao:talonet:2165165", "certificate": JSON_certificate}'
```

Example of a JSON_certificate :

```
{
  "project_title" : "Ligne de production moteur NFG-1000",
  "project_description" : "Conception, réalisation et installation d'une nouvelle␣
↪ligne de production",
  "project_budget" : "2000000",
  "project_staff" : "12",
  "project_location" : "Bordeaux",
  "start_date" : "2019-02-22",
  "end_date" : "2020-01-25",
  "competencies" : ["CATIA V6",],
  "score_recommendation" : 4,
  "score_delivery" : 3,
  "score_schedule" : 4,
  "score_communication" : 4,
  "score_budget" : 4,
 }
```

14.6 Endpoint : POST https://talao.co/api/v1/issue_agreement

Issue an agreement certificate to a company. Your company must be in the company's referent list.

Scope required client:issue:agreement.

Issue an agreement :

```
$ curl -X POST https://talao.co/api/v1/issue_agreement_on_behalf  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"did" : "did:talao:talonet:2165165", "certificate": JSON_certificate}'
```

Example of a JSON_certificate:

```
{
  "registration_number" : "2020-11-31003",
  "title" : "IQ - ISO9001:2020",
  "description" : "Quality Management Process",
  "standard" : "ISO 9001",
  "date_of_issue" : "2020-11-01",
  "valid_until" : "2030-10-31",
  "location" : "Toulouse Bordeaux Paris",
```

(continues on next page)

(continued from previous page)

```
  "service_product_group" : "Drone Serie production line",
}
```

14.7 Endpoint : POST https://talao.co/api/v1/update_identity_settings

to be done

14.8 Endpoint : POST https://talao.co/api/v1/get_certificate_list

Get the certificate list of an Identity. Your company must be in the partner list.

certificate_type is : “experience”, “skill”, “agreement”, “reference”, “recommendation” or “all”.

No scope required.

```
$ curl -X POST https://talao.co/api/v1/get_certificate_list  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"did" : "did:talao:talonet:2165165", "certificate_type": "reference"}'
```

Example of a JSON return :

```
{
  "certificate_list" : [
↪"did:talao:talaonet:b8a0a9eE2E780281637bd93C13076cc5E342c9aE:document:6",
   "did:talao:talaonet:b8a0a9eE2E780281637bd93C13076cc5E342c9aE:document:12"]
}
```

14.9 Endpoint : POST https://talao.co/api/v1/get_certificate

Get certificate data. Your company must be in the partner list of the Identity.

No scope required.

```
$ curl -X POST https://talao.co/api/v1/get_certificate  \
 -H "Authorization: Bearer rp9maPLRQEJ3bviGwTMPXvQdcx8YlqONuVDFZSAqupDdgXb9" \
 -H "Content-Type: application/json" \
 -d '{"certificate_id" :
↪"did:talao:talaonet:81d8800eDC8f309ccb21472d429e039E0d9C79bB:document:12"}'
```

Example of a JSON return :

```
{
  "created": "2020-09-28 14:37:59",
  "data_location": "https://gateway.pinata.cloud/ipfs/
↪QmWrsG2RSVmJFpLsfwHJttv4DC7RhdN5oxnsJ3k5EVh7cP",
  "description": "D\u00e9veloppement d'un application web d\u2019acc\u00e8s au␣
↪protocole Talao permettant de mettre en oeuvre toutes les fonctionnalit\u00e9s du␣
↪protocole et en particulier la gestion des cl\u00e9s priv\u00e9es, les partenariats␣
↪et le cryptage des donn\u00e9es.",
```

(continues on next page)

(continued from previous page)


```
  "doc_id": 12,
  "doctype": 20000,
  "doctypeversion": 2,
  "end_date": "2020-07-30",
  "expires": "Unlimited",
  "id": "did:talao:talaonet:81d8800eDC8f309ccb21472d429e039E0d9C79bB:document:12",
  "identity": {
    "address": "0xE474E9a6DFD6D8A3D60A36C2aBC428Bf54d2B1E8",
    "category": 1001,
    "id": "did:talao:talaonet:81d8800eDC8f309ccb21472d429e039E0d9C79bB",
    "workspace_contract": "0x81d8800eDC8f309ccb21472d429e039E0d9C79bB"
  },
  "ipfshash": "QmWrsG2RSVmJFpLsfwHJttv4DC7RhdN5oxnsJ3k5EVh7cP",
  "issuer": {
    "address": "0xEE09654eEdaA79429F8D216fa51a129db0f72250",
    "category": 2001,
    "id": "did:talao:talaonet:4562DB03D8b84C5B10FfCDBa6a7A509FF0Cdcc68",
    "name": "Talao",
    "workspace_contract": "0x4562DB03D8b84C5B10FfCDBa6a7A509FF0Cdcc68"
  },
  "logo": "Qme3vLZP6n8xNQj6qmL8piGyWVUhm4oYhmYXMqvczzN3Z1",
  "manager": "Director",
  "privacy": "public",
  "reviewer": "",
  "score_communication": "4",
  "score_delivery": "4",
  "score_recommendation": "4",
  "score_schedule": "4",
  "signature": "QmdMBfNut5GosNKrN73GhncbvkWqGLLNZJR5omEpAi9bkD",
  "skills": [
    "Blockchain",
    " Solidity",
    " Talao",
    " ERC725",
    " Python"
  ],
  "start_date": "2020-03-01",
  "title": "Project Leader",
  "topic": "certificate",
  "transaction_fee": 1000000000000,
  "transaction_hash":
↪"0x0e4600aab98d171078509f51bb12b1d16def8574f57251c1fc94a9b5e7cf66ca",
  "type": "experience",
  "version": 1
}
```

CHAPTER 15

Features

15.1 Basic

- Créér son identité (personne)
- Mettre à jour son CV
- Demander une preuve d'identité à Talao
- Utiliser son wallet pour gérer son identité (en cours de dev)

15.2 Certification

- Nommer un référent : Donner une autorisation d'emettre des certificats a une personne ou une entreprise qui a une identité
- Demander un certificat à un référent (persone ou entreprise)
- Demander un certificat à une personne qui n'a pas d'identité. La création de l'identité est automatisée dans le process d'émission du certificat
- Certifier une personne qui a une identité.

15.3 Partage de données

- Stocker des données et des fichiers cryptés/non-cryptés
- Nommer un partenaire : Donner l'acces à de l'information cryptée à une personne ou une entreprise qui a une identité

15.4 Divers

- Tracer un certificat
- Créer un lien pour un accès public à un certificat
- Créer un lien pour un accès public à une identité
- Emettre des certificats d'expérience et des recommendations
- Inviter une personne à créer son identité
- Consulter un Dashboard
- Obtenir des Rewards (en cours de dev)
- Gérer son compte (password, telephone, signature, photo, eth et token,. . .)
- Accéder à un site adpté à son device (Responsive Web Design)
- Accéder à une aide en ligne

15.5 Reservé à Talao

- Créer l'identité d'une entreprise
- Emettre une preuve d'identité pour une persone ou une entreprise
-

CHAPTER 16

Internal

16.1 Name Service (NS)

Name Service (NS) is an independant routine to provide a readable identifier for DID and an easy way to log to company and person Identity through Relay. One can use NS to setup Manager for companies. THe Managers have the right to use the Relay to sign transaction on behalf of the Identity.

It supports :

- Identity_name : a readable name for a DID (an identity workspace contract).
- Alias Name : for a person it is a readable name to log its own identity an an email to authentify.
- Manager Name : a readable name/email to log to a company identity.

Manager have a username made up of 2 parts example 'johndoe.generalmotors". A manager MUST have is own identity. Identity and Alias are one part names : "johndoe"

At Identity creation, 2 statements are written :

- in the Resolver Table (identity_name/identity_workspace_contract/date)
- in the Alias Table (alias_name/identity_name/email/date).

At Manager creation, one stament is written :

- in the Manager Table of the company (manager_name/alias_name/email/date).

To log to the company Identity through Relay the manager will use a 2 parts username as "manager_name.company_identity_name".

NS is today supported by SQLite3 with one DB per company for Managers and one DB for DID, Publickey and Alias (Migration to a decentralied support in progress).

16.2 IPFS

We use IPFS and Pinata pin services for data persistence.

To add data to IPFS we first add to PInata Node and pin to local node. To get data , we first get from local and after timeout of 5s we get from pinata. Our Pin Policy at Pinata is to have 2 replications in Europe.

16.3 Identity vs keys

Company Identities are always created by Talao which has a copy of the private key and RSA key

For User Identity, it depends on the way it has been created. Talao might have nothing or only a Management key to sign transactions or a Management Key + RSA key or the private key. If user Identity has been created by Relay, Talao has a copy of the private key, RSA key and secret key.

16.4 Talao ERC725 Keys

Keys	Usage
1	Relay if activated
2	Not Used
3	Personal/Company settings/did_auth
4	Not used
5	Issuer White List
20002	Issuer Documents
20003	Not used

16.5 Talao Documents

JSON format is used to organized data within Talao Documents.

Read more technical information on Talao Documents.

16.5.1 Doctype

One document is defined through is 'doctype' (int). A document can be **Public**, **Private** or **Secret**. By default most documents are Public.

doctype	Public	Private	Secret
kbis	10000	N/A	N/A
kyc	15000	15001	N/A
certificate	20000	N/A	N/A
education	40000	40001	40002
experience	50000	50001	50002

CHAPTER 17

JSON data structure

17.1 Kbis


```
{
"siren" : "662 042 449",
"date" : "1966-09-23",
"name" : "BNP",
"legal_form" : "SA",
"naf" : "6419Z",
"capital" : "2 499 597 122 EUROS",
"address" : "16 BOULEVARD DES ITALIENS, 75009 PARIS",
"activity" : "Servics financiers",
"ceo" : null,
"managing_director" : null
}
```


17.2 Kyc (OpenId Connect scope) ERC725


```
{
"identification" : "Face to Face check",
"email" : "",
"phone" : "",
"family_name" : "Houlle",
"given_name" : "Pierre david",
"gender" : "M",
"birthdate" : "1980-1212",
"address" : ""
}
```

17.3 Certificates

```
{
"type" : "experience",
"version" : 1,
"title" : "Chef de projet Blockchain",
"description" : "Conception et ralisation d un prototype Ethereum d un suivi de␣
↪production",
"start_date" : "2018/02/22",
"end_date" : "2019/01/25",
"skills" : ["Ethereum", "Solidity"],
"score_recommendation" : 2,
"score_delivery" : 3,
"score_schedule" : 4,
"score_communication" : 4,
"logo" : "thales.png",
"signature" : "permet.png",
"manager" : "Jean Permet",
"reviewer" : "Paul Jacques"
}
```

```
{
"type" : "reference",
"version" : 1,
"title" : "",
"description" : "",
"budget" : "",
"staff" : "",
"location" : "",
"start_date" : "2018-02-22",
"end_date" : "2019-01-25",
"competencies" : ["", ""],
"score_recommendation" : 2,
"score_delivery" : 3,
"score_schedule" : 4,
"score_communication" : 4,
"score_budget" : 4,
"issued_by" : {
        "name" : "",
        "postal_address" : "",
        "siren" : "",
        "logo" : "xxx",
        "signature" : "xxx",
        "manager" : ""
        }
"issued_to" : {
        "name" : "",
        "postal_address" : "",
        "siren" : "",
        "logo" : "",
        "signature" : "",
        }
}
```

Score is an integer value [0,1,2,3,4,5] for 5 evaluations :

- How satisfied are you with the overall delivery ?

- How would you rate his/her ability to deliver to schedule ?
- How would you rate its communication ?
- How would you rate its ability to stay within the set budget?
- How likely are you to recommand this company ?

```
{
"type" : "agreement",
"version" : 1,
"registration_number" : "xxx",
"title" : "xxx",
"description" : "xxx",
"standard" : "",
"date_of_issue" : "xxx",
"valid_until" : "xxx",
"location" : "xxx",
"service_product_group" : "xxx",
"issued_by" : {
        "name" : "",
        "postal_address" : "",
        "siren" : "",
        "logo" : "xxx",
        "signature" : "xxx",
        "manager" : "",
        }
"issued_to" : {
        "name" : "",
        "postal_address" : "",
        "siren" : "",
        "logo" : "",
        "signature" : "",
        }
}
```

```
{
"type" : "recommendation",
"version" : 1,
"description" : "",
"relationship" : ""
    }
```

```
    {
"type" : "skill",
"version" : 1,
"title" : "",
"description" : "",
"date_of_issue" : "",
"logo" : "",
"signature" : "",
"manager" : "",
"reviewer" : ""
    }
```

17.4 Experience

```
{
"company" : {
        "contact_email" : "Pierre@bnp.com",
        "name" : "Thales",
        "contact_name" : "Jean Dujardin",
        "contact_phone" : "0607254589"
                        },
"title" : "Chef de projet Blockchain",
"description" : "Conception et ralisation d un prototype Ethereum d un suivi de␣
↪production",
"start_date" : "2018/02/22",
"end_date" : "2019/01/25",
"skills" : ["Ethereum", "Solidity"],
"certificate_link" : ""
}
```

17.5 Education

```
{
"organization" : {"contact_email" : "Pierre@bnp.com",
        "name" : "Ensam",
        "contact_name" : "Jean Meleze",
        "contact_phone" : "0607255656"},
"title" : "Master Engineer",
"description" : "General Study",
"start_date" : "1985/02/22",
"end_date" : "1988/01/25",
"skills" : [],
"certificate_link" : ""
}
```