
Talao Professional Identity Relay

Release 0.7.9

Read the Docs, Inc & contributors

May 27, 2021

CONTENTS:

1	Overview	1
1.1	What is Talao ?	1
1.2	How does Talao work ?	1
1.3	TalaoNet	2
1.4	Credits	2
2	Privacy	3
2.1	Overview about encryption and privacy	3
2.2	Two-factors authentication	5
2.3	Data and privacy	5
3	Professional Identity	7
3.1	Personal settings	7
3.2	Proof of Identity	7
3.3	Experience	7
3.4	Education	8
3.5	Certificates	8
3.6	Alias	8
3.7	Referent	8
3.8	Partner	9
3.9	White List	9
3.10	Data Store	9
3.11	Advanced	9
4	Quick Start	11
4.1	Setup	11
4.2	Login	11
4.3	Short Message Authentificaton	12
4.4	Support	12
5	Request a Certificate	13
5.1	Types of Certificates	13
5.2	Experience Certificates	13
5.3	Recommendations	14
6	Get Rewards (in progress)	15
7	Add a Referent	17
8	Use my own Ethereum Address	19

9	Get a Proof of Identity	21
10	APIs	23
10.1	Data Request and Response	23
10.2	Exchange data with User	26
11	Workflows	29
11.1	Basic	29
11.2	Certification	29
11.3	Partage de données	29
11.4	Divers	29
11.5	Reservé à Talao	30
12	Internal	31
12.1	Name Service (NS)	31
12.2	IPFS	32
12.3	Identity vs keys	32
12.4	Talao ERC725 Keys	32
12.5	Talao Documents	32
13	Organisation des tests (terminés au 30/07/2020)	35
13.1	Contexte	35
13.2	Objectif des tests	36
13.3	Equipe de testeurs et projet de test	36
13.4	Environnement technique	36
13.5	Démarche pour les testeurs	36
13.6	Base de test	37

OVERVIEW

1.1 What is Talao ?

Talao is a Blockchain protocol to manage professional data.

Traditional architectures to validate, certify, and manage professional data are based on centralized, top-down approaches that rely on third-party private operators. Unfortunately this organization often leads to inappropriate use of personal data and hacks.

Talao approaches this problem starting from a user perspective through a Blockchain decentralized Identity focused on professional data :

- You own your data for your lifetime.
- No private operators or government agencies can decide to update or delete your data.
- No one can access your encrypted data without your permission.
- No storage costs, you only pay Blockchain fees to update your data.
- Certificates are tamper proof and traceable.
- Certificates issuers are identified.

Talao allows professional data certification for Talents, Companies and other organizations 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 certificates can be displayed anywhere on digital platforms : social medias, websites, Jobboards, etc. They provide to third parties reliable data about professional experiences, skills and education.

1.2 How does Talao work ?

Talao is based on smart contracts Identities, it means that individuals and companies must first setup their own private smart contract (program) on the Blockchain to store and manage their data. 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. Those keys are never stored in a database. If someone wants to update his data, he will sign a message (data update) with his private key and send it to thousands of Blockchain servers. Each server will check the signature, update its data then compare it to other servers. As Blockchain data are duplicated on thousands of servers, no one can alone hack the Identity.

This Talao web application (named Relay) is a portal to access Identities with a simple User Interface and automated processus.

1.3 TalaoNet

TalaoNet is a Private Ethereum Network with a Proof Of Authority consensus (Clique) managed by Talao and partners. The Talao protocol has been deployed on TalaoNet.

RPC URL <http://18.190.21.227:8502>

Main contract addresses

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

1.4 Credits

Thanks to the awesome Ethereum community which provide us with great tools, Solidity code and inspiration. 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 library [NLTK](#). For more information Bird, Steven, Edward Loper and Ewan Klein (2009), Natural Language Processing with Python. O'Reilly Media Inc.

PRIVACY

2.1 Overview about encryption and privacy

An Identity is a smart contract on the Ethereum Blockchain, it 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 2 specific AES encryptions keys (one for private data, one for secret data) to encrypt user data. Those 2 keys are stored within the Identity encrypted with a RSA key.

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

- If the Identity has been setup by the Relay itself, the Relay 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 owner**. All services are available through the Relay which is a classic webserver application.
- If the Identity has been setup by the user externally (see [freepdapp](#)), the Relay is **Fully or partially activated** (with ERC725 Keys) to be able to sign transactions on behalf of the owner. In this case the Relay does not have a copy of the Ethereum private and RSA keys but the user has limited access to the Relay services. For instance certificate issuance and Partnership services are not available.
- An other solution is to do a **Change of ownership** : The Identity is setup by the Relay and later on the Identity is transferred to an Ethereum address setup secretly by the owner. In this case the Relay does not have a copy of the Ethereum private key. This solution has the advantage to not requiring the setup of an Identity externally. Certificate issuance services are not available.

For information company Identities are always managed on behalf of the company as they usually do not want to be involved in those tasks.

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 Relay Services :

- Request certificates,
- Edit personal settings,
- Edit resume (Experience, Education, ...)
- Issue certificates,
- Manage Partnership,
- Manage Alias,

- Manage Referent,
- Manage White List,
- Store files.

Mode	Priv.key	RSA Key	Services and Relay rights
Managed on behalf of the owner	<ul style="list-style-type: none">• Relay has copy	<ul style="list-style-type: none">• Relay has copy	<ul style="list-style-type: none">• User can access all services through Relay• Relays has acces to all data
Fully activated (Key=1)	<ul style="list-style-type: none">• Secret	<ul style="list-style-type: none">• Secret	<ul style="list-style-type: none">• User cannot issue certificates• Relay can edit personal settings and resume• Relay can add Referent and Alias• Relay can issue public data
Partially activated (key=20002)	<ul style="list-style-type: none">• Secret	<ul style="list-style-type: none">• Secret	<ul style="list-style-type: none">• User cannot issue certificates• User cannot edit Resume and personal settings• User cannot add Alias and Referent• User cannot manage partnership• Relay can edit Resume
Change of ownership	<ul style="list-style-type: none">• Secret	<ul style="list-style-type: none">• Relays has copy	<ul style="list-style-type: none">• User cannot issue certificates• Relays has access to all data

2.2 Two-factors authentication

For security this web application uses a two-factors authentication protocol.

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.

Warning: Those 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](#) .

- By default for Talents, Contact Email and Contact Name are private.

Secret Data are only available for users.

- Users can store encrypted data on decentralized support as IPFS through this option.
- Authentication Email is always secret (Relay keeps a copy of ths email for authentication)

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 Identi 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 standard 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 Training 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 authentication through the [Relay](#)

At setup, one smart contract is created for each identity and one authentication 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. Unfortunately this 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 your 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 authorisation 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 eventually 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 first 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 useful 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 Relay 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 of 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 create Private or Secret data.

QUICK START

You can access to this Guide trough the navigation bar if you use a large device screen or through the right dropdown menu on your smartphone.

4.1 Setup

- Go to <http://talao.co/starter/>
- Choose the “Quick Start” option (first option) to create a new Professional Identity
- Enter firstname, lastname and an email for authentication purpose. Your firstname and lastname will be public, your email will be encrypted and used only for authentificaion.

Note: This email is encrypted and only used for authentication in the early process. it wont be displayed to public. Later on you will get options to setup public emails for contact. Read more in *Professional Identity*.

The process to create an Identity will take a couple of minutes depending of the load of the Ethereum Network. A username will be setup based on your firstname and lastname and you will receive an email with all information and cryptographic keys of your Identity. In particular store your Private Key and RSA Key secretly.

Warning: Never use your Identity Ethereum address to store crypto money (ETH or others). Best option is to use cold wallet for funds with speciific Ethereum addresses.

4.2 Login

- Go to <http://talao.co> and enter you username .Your will receive a dynamic password by email.
- Check your email and enter the password (3 trials maximum, 3 minutes maximum). Your are logged.
- Complete your profil as much as possible and request certificates to Companies or Individuals. Read more in *Request a Certificate*

4.3 Short Message Authentificaton

By default secret codes for authentication are sent by email, but you can configure your profil to receive secret codes by Short Message. To set up this option go to the “Advanced” menu of your profile, scroll down and and clic on “Add or update your phone number for authentication”. If you want to remmove this option and receive secret codes by email, leave the field blank.

4.4 Support

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

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 <http://talao.co/register/> and enter your firstname, lastname and an email for authentication.
- When you receive your username and private keys go to <http://talao.co> to log and access your Identity
- Then click 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 will 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 employee or you can delete it.

In order to strengthen your Certificate best is to get a Proof of the Issuer Identity and yours. See Next.

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 employee or you can delete it.

GET REWARDS (IN PROGRESS)

You can get rewards in TALO tokens depending of your involvement. 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 authentication 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

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 Identity 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.

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 access your Identity. However the limitations are :

- you will not be able to 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 manage 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, contact 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 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”.

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 Identity 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 authentication email to contact@talao.io.

The Talent Connect APIs are a set of APIs to get public data of a Professional Identity (Talent or Company) to eventually start an onboarding process.

For companies it is an easy way to get reliable data about Talents.

For Talents it is an efficient way to expose their true skills and personal credentials while controlling their data.

Each parcel of data can be explored to get

- issuer information, signature, name,
- date of creation and expiration,
- data location,
- proofs of validity.

10.1 Data Request and Response

10.1.1 General Request

```
GET http://talao.co:5000/api/v1/talent-connect/
```

10.1.2 Header

```
"Content-Type: application/json"
```

10.1.3 Payload

- user
 - a username or a Decentralized IDentifiant
- topicname
 - for a person : firstname, lastname, contact_email, contact_phone, birthdate, postal_address (self declared)
 - for a company : name, contact_name, contact_phone, contact_email, website (self declared)
 - resume : full resume of a user
 - analysis : resume data analysis

- kyc or kbis (issued by third parties)
- experience : list of all experiences (self declaration)
- certificate : list of all certificates issued by third parties
- education : list of diplomas (self declaration)
- search : (to be completed)
- option (optional)
 - to be completed

10.1.4 Example

```
$ curl -GET http://talao.co:5000/api/v1/talent-connect/ \
-H "Content-Type: application/json" \
-d user=jean.pascalet \
-d topicname=experience
```

10.1.5 Response

```
[
{
  "topic": "experience",
  "created": "2020-05-25 10:07:22",
  "issuer": {
    "address": "0x18bD40F878927E74a807969Af2e3045170669c71",
    "workspace_contract": "0xD6679Be1FeDD66e9313b9358D89E521325e37683",
    "category": 2001,
    "id": "did:talao:rinkeby:D6679Be1FeDD66e9313b9358D89E521325e37683",
    "name": "Relay",
    "contact_name": null,
    "contact_email": null,
    "contact_phone": null,
    "website": null
  },
  "transaction_hash": "0x49dc98ad487a33a4e066e8e05758870e7972466c5e74c261ea5b4ebe091003de",
  "transaction_fee": 20000000000000,
  "doctypeversion": 2,
  "ipfshash": "QmThxo5shaJSDCYZprXzwknqgCoPja5rUW3528qNFHCKft",
  "data_location": "https://gateway.ipfs.io/ipfs/QmThxo5shaJSDCYZprXzwknqgCoPja5rUW3528qNFHCKft",
  "expires": "Unlimited",
  "privacy": "public",
  "doc_id": 23,
  "id": "did:talao:rinkeby:Ec0Cf3FA4158D8dd098051cfb14af7b4812d51aF:document:23",
  "identity": {
    "address": "0x048D19e72030a9D7a949517D5a9E3844b4533fc2",
    "workspace_contract": "0xEc0Cf3FA4158D8dd098051cfb14af7b4812d51aF",
    "category": 1001,

```

(continues on next page)

(continued from previous page)

```

    "id": "did:talao:rinkeby:Ec0Cf3FA4158D8dd098051cfb14af7b4812d51aF"
  },
  "title": "CTO",
  "description": "En charge du projet Blockchain",
  "end_date": "2020-05-01",
  "start_date": "2020-01-01",
  "company": {
    "address": null,
    "contact_email": "basil@bnp.com",
    "contact_name": "",
    "contact_phone": "0607182594",
    "name": "BNP",
    "website": null,
    "workspace_contract": null
  },
  "certificate_link": null,
  "skills": [
    "Java"
  ]
},
{
  "topic": "experience",
  "created": "2020-06-06 18:54:35",
  "issuer": {
    "address": "0x18bD40F878927E74a807969Af2e3045170669c71",
    "workspace_contract": "0xD6679Be1FeDD66e9313b9358D89E521325e37683",
    "category": 2001,
    "id": "did:talao:rinkeby:D6679Be1FeDD66e9313b9358D89E521325e37683",
    "name": "Relay",
    "contact_name": null,
    "contact_email": null,
    "contact_phone": null,
    "website": null
  },
  "transaction_hash": "0xb3c181a2490ebf9a18e875cbb47e14041c5f7a34854cd8e9ca9f2016d092696c",
  "transaction_fee": 20000000000000,
  "doctypeversion": 2,
  "ipfshash": "QmdWCKBVybPRQvWmY7hAbkRHFRXvvPPqKAi8ieZBm2WtEd",
  "data_location": "https://gateway.ipfs.io/ipfs/
  ↪ QmdWCKBVybPRQvWmY7hAbkRHFRXvvPPqKAi8ieZBm2WtEd",
  "expires": "Unlimited",
  "privacy": "public",
  "doc_id": 36,
  "id": "did:talao:rinkeby:Ec0Cf3FA4158D8dd098051cfb14af7b4812d51aF:document:36",
  "identity": {
    "address": "0x048D19e72030a9D7a949517D5a9E3844b4533fc2",
    "workspace_contract": "0xEc0Cf3FA4158D8dd098051cfb14af7b4812d51aF",
    "category": 1001,
    "id": "did:talao:rinkeby:Ec0Cf3FA4158D8dd098051cfb14af7b4812d51aF"
  },
  "title": "CTO",

```

(continues on next page)

(continued from previous page)

```

    "description": "We are working to deliver software solutions and consulting services.
    ↳to businesses worldwide, and help our clients to create innovative and technological.
    ↳products in various areas.\r\n\r\nInnowise Group team is divided into several.
    ↳departments and structural units responsible for certain areas of company\u2019s.
    ↳activities.\r\nSeamless collaboration between all of them on a daily basis helps us.
    ↳achieve short term objectives and strategic goals.",
    "end_date": "2019-11-01",
    "start_date": "2019-07-01",
    "company": {
      "contact_email": "pierre@bnp.com",
      "contact_name": "Pierre",
      "contact_phone": "01 607182594",
      "name": "Covea"
    },
    "certificate_link": "",
    "skills": [
      "Business",
      "Management,",
      "consulting"
    ]
  }
]

```

10.2 Exchange data with User

10.2.1 General Request

Authenticating using a login and secret through HTTP Basic Authentication. Check your your API credentials.

Access can be also secured through a specific White List to limit the client domains.

```
POST http://talao.co:5000/api/v1/talent-connect/auth/
```

10.2.2 Header

```
"Content-Type: application/json"
```

10.2.3 Authentication

```
login:secret
```

10.2.4 Payload

```
{"action" : xxxx, "user" : xxxxx}
```

action :

- call_back : send an email
- to be completed

10.2.5 Example

```
curl -X POST http://192.168.0.34:3000/talent-connect/auth/ \
-u 0x4A2B67f773D30210Bb7C224e00eAD52CFCDf0Bb4:3042d4704a513b3ffb4a2adb78e73446 \
-d '{"action" : "call_back"}' \
-H "Content-Type: application/json"
```


WORKFLOWS

11.1 Basic

- Créer 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)

11.2 Certification

- Nommer un référent : Donner une autorisation d'émettre des certificats à une personne ou une entreprise qui a une identité
- Demander un certificat à un référent (personne 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.

11.3 Partage de données

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

11.4 Divers

- Tracer un certificat
- Créer un lien pour un accès public à un certificat
- Créer un lien pour un accès public à une identité
- Émettre des certificats d'expérience et des recommandations
- 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 adapté à son device (Responsive Web Design)
- Accéder à une aide en ligne

11.5 Réservé à Talao

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

12.1 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).

```
def init():
    conn = sqlite3.connect('nameservice.db')
    cur = conn.cursor()
    cur.execute('create table alias(alias_name text, identity_name text, email text,
↳date real)')
    cur.execute('create table resolver(identity_name text, identity_workspace_
↳contract text, date real)')
    cur.execute('create table publickey(address text, key text)')
    conn.commit()
    cur.close()
    return
```

(continues on next page)

(continued from previous page)

```
def init_host(host_name) :
    conn = sqlite3.connect(host_name + '.db')
    cur = conn.cursor()
    cur.execute('create table manager(manager_name text, alias_name text, email text, ↵
↵date real)')
    conn.commit()
    cur.close()
```

12.2 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.

12.3 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.

12.4 Talao ERC725 Keys

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

12.5 Talao Documents

JSON format is used to organized data within Talao Documents.

Read more technical information on [Talao Documents](#).

12.5.1 Doctype

One document is defined through its '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	N/A	N/A
certificate	20000	N/A	N/A
education	40000	40001	40002
experience	50000	50001	50002

12.5.2 Kbis

```
{ "siret" : "662 042 449 00014",
  "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" : "Services financiers",
  "ceo" : null,
  "managing_director" : null}
```

12.5.3 Kyc

```
{"country" : "FRA3",
  "id" : "15CA98225",
  "lastname" : "Houille",
  "firstname" : "Pierre david",
  "sex" : "M",
  "nationality" : "Francaise",
  "date_of_birth" : "1980-12-12",
  "date_of_issue" : "2012-02-13",
  "date_of_expiration" : "2022-02-12",
  "authority" : "Prefecture de Police de Paris",
  "card_id" : "xxxxxxxxx"}
```

12.5.4 Certificate

```
{"type" : "experience",
  "title" : "Chef de projet Blockchain",
  "description" : "Conception et réalisation d un prototype Ethereum d un suivi de_
  ↪production",
  "start_date" : "2018/02/22",
  "end_date" : "2019/01/25",
  "skills" : ["Ethereum", "Solidity"],
```

(continues on next page)

(continued from previous page)

```
"score_recommendation" : 2,
"score_delivery" : 3,
"score_schedule" : 4,
"score_communication" : 4,
"logo" : "thales.png",
"signature" : "permet.png",
"manager" : "Jean Permet",
"reviewer" : "Paul Jacques"}
```

12.5.5 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" : ""}
```

12.5.6 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" : ""}
```

ORGANISATION DES TESTS (TERMINÉS AU 30/07/2020)

13.1 Contexte

Le protocole Talao est une application de la blockchain Ethereum permettant la gestion d'Identités Décentralisées spécialisées sur les données professionnelles. Cf ce [lien](#) pour plus d'information sur les Identités Décentralisées. Les principaux apports du protocole sont :

- la protection des données personnelles pour les utilisateurs,
- la fiabilité et la traçabilité des données RH pour l'entreprise,
- la possibilité d'émettre des certificats infalsifiables et inaltérables en quelques minutes avec des frais minimum.

Une première version du protocole Talao a été déployée en Février 2018. Il a été installé avec un accès utilisateur sous la forme d'une [Dapp](#). Suite à ce déploiement l'équipe Talao s'est concentrée sur la commercialisation de l'offre en B2B auprès des grands comptes sur le secteur des freelances représentant un "use case" relativement simple. Plusieurs projets ont été initiés en particulier pour l'émission de certificats pour des entreprises du secteur des ESN qui trouvaient dans un contexte de pénurie de ressources et de fort turn over de leurs personnels un outil de renforcement de leur marque employeur.

Dans ce contexte nous avons en revanche constaté que la mise en œuvre de la Dapp et en particulier son adoption par des utilisateurs non experts était difficile compte tenu de la complexité des manipulations. Il faut aujourd'hui pour utiliser le protocole non seulement disposer d'un wallet Ethereum et de cryptos mais aussi d'être en mesure de signer des transactions Ethereum avec un outil tel que Metamask.

Compte tenu de la période actuelle propice à de nouveaux projets en entreprise, l'équipe Talao s'est donc investie sur la réalisation d'une nouvelle solution technique pour l'accès simplifiée des utilisateurs au protocole dans le but d'initier un déploiement en B2C.

Cette solution est construite autour d'une **application web centralisée** traditionnelle permettant une simplification maximum de la gestion de son Identité en contre-partie de l'introduction d'une intermédiation plus ou moins importante Cf [Privacy](#).

Cette application a été définie autour du concept de la **gestion pour compte de tiers de l'Identité**. C'est cette nouvelle application qui fait l'objet de ces tests.

13.2 Objectif des tests

Il s'agit de :

- vérifier la valeur ajoutée des fonctionnalités proposées aux utilisateurs,
- de s'assurer de la facilité de leur mise en oeuvre,
- d'identifier des points d'amélioration (contenu et design),
- de relever les bugs existants.

Le scope du test est :

- l'application web <http://talao.co:5000/starter/>
- Cette documentation (dans sa partie user hors Talent Connect et Internal)

13.3 Equipe de testeurs et projet de test

L'équipe de test est constituée de 5 personnes maximum, la durée des tests est prévue sur environ 15 jours courant juillet 2020.

Note: Les testeurs s'engagent sur l'honneur à conserver la confidentialité de ce projet et en particulier de s'abstenir de diffuser des informations concernant ces tests sur les réseaux sociaux sans l'accord de Talao. Talao pourra interrompre ces tests à tout moment de sa propre initiative si nécessaire.

13.4 Environnement technique

L'application est actuellement installée sur un serveur AWS et fonctionne sur la blockchain de test Rinkeby. Les tokens TALAO et ETH utilisés sur Rinkeby n'ont pas de valeur marchande.

L'application est accessible au travers d'un browser standard (Chrome, IE, Firefox, safari, ...) à partir d'un Smartphone, tablette, PC.

Les problèmes rencontrés sont à documenter sous la forme d'**issues** sur le repository <https://github.com/thierrythevenet1963/Talao>. Pour cela il faudra ouvrir un compte sur <https://github.com/>. C est gratuit.

La mise à jour de l'application en production est faite habituellement sur une base quotidienne (20h00).

13.5 Démarche pour les testeurs

Il n'est pas prévu de plan de test particulier pour les testeurs qui sont libres de manipuler l'application en fonction de leur disponibilité et de leur curiosité.

Nous leur conseillons en revanche :

- de commencer par la lecture de cette documentation et en particulier des chapitres How-To et Quick Start,
- de commencer par explorer la base de test,
- de créer leur propre identité,

- de limiter la demande de certificats (par email) à 1 ou 2 personnes connues, sachant que systématiquement une identité sera créée pour chacune de ces personnes si celles-ci acceptent d'émettre le certificat.

Note: Toutes les informations, images, etc de la base de test actuelle correspondent à des utilisateurs et des sociétés fictives meme si les noms sont parfois connus.

13.6 Base de test

user :

- username : "pascalet", code "123456" : pascalet (Jean Pascalet) a comme référent "jean"
- username : "jean", code "123456" : jean (Jean Pierre Roulle) a comme referent BNP, pascalet, jeanpierrevalga. Jean est manager chez BNP
- username : "thierry" code "123456" : thierry (Thierry Thevenet) est manager chez Talao
- username : "jeanpierrevalga" code "123456" : jeanpierrevalga (Jean Pierre Valga)

entreprise :

- username : "bnp", code "123456" : bnp (BNP) a comme manager jean et comme partner thales et talao
- username : "talao" code "123456" : talao (Talao) a comme manager thierry. Talao dispose de fonctionnalités étendues pour emettre des "proof of identity" (kbis et kyc) et creer des identités.
- username : "thales" code "123456"
- username : "orange" code "123456"

Note: Un manager qui veut accéder à l'identité de la société dont il est manager doit se connecter avec un username double "person.company". Exemple "jean" peut se connecter à l'identité "bnp" avec son username "jean.bnp".
