Talao Professional Identity Relay

Release 0.6

Read the Docs, Inc & contributors

Aug 30, 2023

CONTENTS:

CHAPTER

ONE

OVERVIEW

1.1 What is Talao ?

Talao is a solution 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 data without your permission.
- Credentials are digitally signed by issuers.
- Identifiers for issuers and users are stored on a blockchain registry.
- Credentials and identifiers are compliant with W3C standards.

Talao allows Professional Identities for Talents, Companies and credentials 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.

Credentials are stored on private devices or displayed anywhere on digital platforms : social medias, websites, Job boards, etc. They provide to third parties reliable data about professional experiences, skills and education.

1.2 How does Talao work ?

That is quite simple, for users you register here with your desktop. A new Identity will be setup and the cryptographic keys will be stored on your computer.

Under the hood, Talao is based on 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 has its own private key to access and update its Identity.

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

This Talao web application https://talao.co is a relay to access Self Sovereign Identities with a simple User Interface and automated processus. From a blockchain perspective, the Identity owner is an account owner.

1.3 What are Verifiable Credentials ?

As defined in the current Credentials specification of W3C1 :

“In the physical world, a credential might consist of:

- Information related to identifying the subject of the credential (for example, a photo, name, or identification number)
- Information related to the issuing authority (for example, a city government, national agency, or certification body)
- Information related to the type of credential this is (for example, a Dutch passport, an American driving license, or a health insurance card)
- Information related to specific attributes or properties being asserted by the issuing authority about the subject (for example, nationality, the classes of vehicle entitled to drive, or date of birth)
- Evidence related to how the credential was derived
- Information related to constraints on the credential (for example, expiration date, or terms of use).

A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts. “

More information available :

- https://www.w3.org/TR/vc-data-model/

1.4 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://www.w3.org/TR/did-core/
- 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

1.5 What blockchains support does Talao use ?

The Talao solution is available with different Self Sovereign Identities and public blockchains :

- Ethereum with the did-ethr method.
- Tezos with the did-tz method with curve secp256k1 (tz2).

We also use :

- did-key with curve secp256k1 for specific use cases.
- did-web (did:web:talao.io:...) with curve secp256k1 and a RSA256 key.

Check the Talao DID Document on the DIF Universal Resolver with Talao DID did:web:talao.co

1.6 Credits

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

Special thanks to Spruce for their implementation of SSI and its wide JSON_LD signing suite for different platforms.

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

CHAPTER

TWO

QUICK START

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

2.1 Register

- go to https://talao.co with your desktop viewer,
- Enter firstname, lastname, email and phone number for authentification purpose.

The process to create a Self Sovereign Identity will take a couple of minutes depending on the load of the Network.

This process will create for you :

- an identity based on the uPort Ethereum method did:ethr
- an identity based on the Tezos method did:tz
- an identity on the Talao DNS based on did:web

In order to keep in mind your login credentials, you will receive a username.

2.2 Login

- Go to https://talao.co, log with your username, ask for a new passwowrd if needed and check your email or phone for the secret code.
- Complete your profil as much as possible and request certificates to Companies or Individuals. Read more in *Request a Credential*

2.3 Support

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

CHAPTER

THREE

REQUEST A CREDENTIAL

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 Credential" of the Menu Bar and follow the process.

Note: To request a Credential, 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.

3.1 Types of Credential

So far there are 3 types of credentials available :

- Professional Experience Credentials
- Recommendations (Person to Person)
- Skill credentials

More to come :

- Training Course and Education credentials

3.2 Professional Experience Credentials

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

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 signed and tamper proof. The credential 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. You can donwload your credential and reuse it in another platform (JSON-LD).

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

3.3 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

FOUR

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

FIVE

ADD A REFERENT (ISSUER)

A Referent is a Company or a Person the user has authorized to issue credentials. 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 credentialsto 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

SIX

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

SEVEN

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

EIGHT

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

NINE

FEATURES

9.1 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)

9.2 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.

9.3 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

9.4 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

9.5 Reservé à Talao

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

CHAPTER

TEN

INTERNAL

10.1 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).

10.2 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.

10.3 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.

10.4 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

10.5 Talao Documents

JSON format is used to organized data within Talao Documents.

Read more technical information on Talao Documents.

10.5.1 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

ELEVEN

JSON DATA STRUCTURE

11.1 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
}
```


11.2 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" : ""
}
```

11.3 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" : "",
        }
```

(continues on next page)

(continued from previous page)

```
}
```

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" : "",
```

(continues on next page)

(continued from previous page)

```
"date_of_issue" : "",
"logo" : "",
"signature" : "",
"manager" : "",
"reviewer" : ""
    }
```

11.4 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" : ""
}
```

11.5 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" : ""
}
```