Token

Transformative impact of disruptive technologies in public services

www.token-project.eu

D1.4: Token Testbed: testing environment for Use Cases

Project full title
Transformative impact of disruptive technologies in public services step

Contract No.
870603

Strategic Objective
SC6-TRANSFORMATIONS-2019

Project Document Number
SC6-TRANSFORMATIONS-2019-870603-WP2-D.1.4

Project Document Date
31.12.2020

Deliverable Type and Security
O - PU

Author

FundingBox, CERTH (Sofia Terzi, Athanasios Kapsalis, Konstantinos Votis)

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

Contents

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

1 Introduction

Executive Summary

The ultimate goal of Token is to develop an experimental ecosystem to enable the adoption of Distributed Ledger Technologies (DLTs) and to prove its value, via highly replicable Use Cases, as a driver for the transformation of public services towards an open and collaborative government model approach.

The services are provided via the Token Platform which offers a developer friendly set of plug-and-play services and open-source components for building decentralized apps and services. The services aim to develop and maintain a Blockchain Platform as a Service Solution for piloting the use of Distributed Ledger Technologies.

The Token Testbed environment has been developed in order to allow developers, initially each of the partners of the Token project developing PUCs, to become familiar with the technology and services provided as well as for testing purposes before moving over to the production environment. In particular the testbed provides a developer portal to create credentials, a wiki with documentation about the services and specific access for testing to the following services: Blockchain Notarization services, Distributed and decentralised storage and, the solution for Self-Sovereign Identities.

About this document

The purpose of this document is to provide the reader with an overview of the testbed environment and its services as well as providing the indications to register in its developer portal to access its services.

Intended Audience

This document will be useful for anyone with a technical background wanting to explore some of the decentralised technologies available through the Token Platform.

Reading recommendations

The document is divided into two main parts:

- A first part describing the testing environment and how to access to it
- An Annex with the description of the 4 blocks of services that will be provided by the Token Platform.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

2 Testbed Environment

The Testbed is a developing and testing environment for the developers to start testing and becoming familiar with the services Token Platform is providing.

Orchestration and deployment of Token Generic Enablers will be done with real life IT resources and adapted security conditions.

This testbed environment will at first only be available to the partners of the TOKEN project.

The Testbed environment is composed of:

- **The Developer Portal** which will be the getaway for the pilots to create their accounts and credentials to access the different services. The developer portal can be accessed via this link. https://developers.token-project.eu/signin
- **Documentation**: the initial documentation related to the services provided (before the wiki is produced in month 12) https://docs.token-project.eu/
- **Testnet**: A Hyperledger Fabric testnet implementing the Notarization Services and API.
- **SSI Testnet:** A Hyperledger Indy testnet implementing the Self-Sovereign Identity Services. The developer services can be accessed at https://ssi.token.iti.gr
- **A IPFS cluster** connected to the IPFS public network, and, implementing a Public Web Gateway, a Pinning service and its APIs
- **An API Gateway** as a wrapper for all the services APIs
- **Tools and Resources**: additional developer tools and resources

The Testbed environment allows the users to create an account and generate the credentials to be able to test the different technologies and services as well as to learn more about each of the services and their potential uses.

To understand their suitability and adherence to developers' needs, the Token Platform services were introduced in the Warm Up Token project bootcamp which took place at the end of October 2020.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

2. 1 Services and Infrastructure

The developer portal will host the services provided by the Token Platform each of them requiring a certain infrastructure. In general terms, the developer portal will provide access to the services that will be run in a private permissioned network.

To access all of such services and for the convenience of the users, an API gateway will be provided. This gateway will wrap the different APIs of the Token services in one socket so that the users of the services just need to connect to one and choose the services they want to have access to instead of having to connect to different individual APIs.

In the following table we mention the Token services, its availability via the testbed and the required infrastructure that will run behind them.

Table 1 - Token Services

Service	Available on Testbed	Infrastructure/Network
Blockchain Notarization services	Yes	Currently the token notarisation services have been developed in Hyperledger Fabric but will also be developed in Ethereum before the end of the year in order to facilitate the move to Alastria **Hyperledger Fabric**: Hyperledger Fabric is a modular blockchain framework that acts as a foundation for developing blockchain-based products, solutions, and applications using plug-and-play components that are aimed for use within private enterprises. **Ethereum** is a global, open-source platform for decentralized applications. **Alastria** is a non-profit association that promotes the digital economy through the development of decentralised ledger technologies/Blockchain.
Decentralised identity. **Token Connect**	No	Token connect, is a simple solution based on decentralised components, to facilitate the authentication of applications and services. It is an Identity Wallet implementing the DID AuthN profile for

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

		OpenID Connect. It allows the user to login in a service with their Decentralized identifier, and allows Relaying Parties to use the Self Issued OpenId Protocol to authenticate the user.
Self-Sovereign identity	No (Available at Custom Testbed)	For the decentralised identity CERTH is providing a solution developed inhouse to the Token project in order to make available to any Token participant to acquire a globally unique Decentralized Identifiers and to enable the backend services provided by public entities to verify these identities. The use of Hyperledger Aries and Hyperledger Indy gives the framework for the SSI services. The sustainability of this service provided by CERTH beyond the project will be explored in WP6 where the business model and the governance model beyond the project will be defined.
Decentralised storage - **Token Storage Network**	Yes	For decentralised storage, a network using IPFS will be set up. IPFS is A peer-to-peer hypermedia protocol designed to make the web faster, safer, and more open.
Messaging and Events Streaming – **Token Streams**	No	For the Token stream, another network will be implemented using the distributed streaming platform Apache Kafka. Apache Kafka is an open-source distributed event streaming platform used by thousands of companies for high-performance data pipelines, streaming analytics, data integration, and mission-critical applications.
Fiware Canis Major	No	Canis Major Blockchain Adaptor: enabling the integration of the Context Broker with multiple blockchains.

2.2 Accessing the Testbed Environment

The Testbed environment main point of access is the Developer Portal, where the user is able to create a developer account and generate the credentials to access the services in place. This portal also contains relevant information about the services provided (see more detail in the Annex).

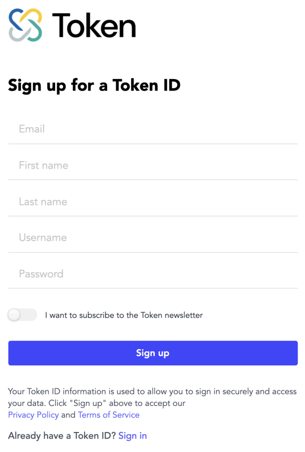
This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

The Developer Portal is the gateway for the pilots to create their accounts and credentials to access the different services.

The Developer portal can be accessed here https://developers.token-project.eu/signin

The following are the steps to register and start using the Developer Portal.

Step 1. Create a developer account.



Token

Sign up for a Token ID

Email

First name

Last name

Username

Password

I want to subscribe to the Token newsletter

Sign up

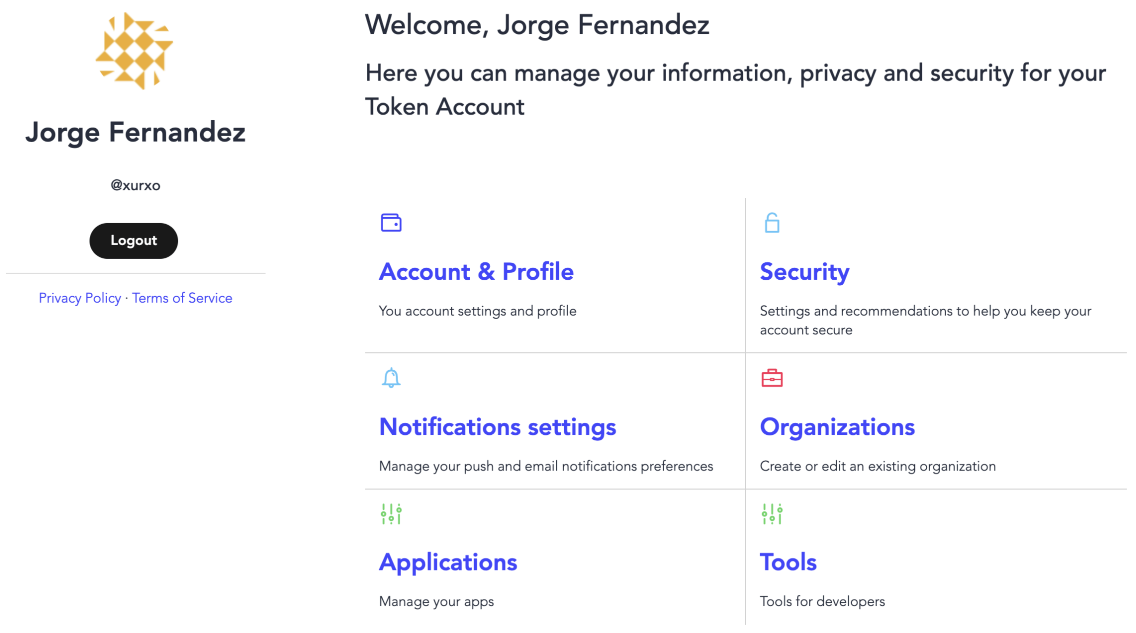
Your Token ID information is used to allow you to sign in securely and access your data. Click "Sign up" above to accept our Privacy Policy and Terms of Service

Already have a Token ID? Sign in

Step 2. Access the dashboard and create an organisation profile.

Organizations profiles allow any user to organize the work based on how they intend to use the Token APIs, so that any user can effectively manage their access to the APIs. Each Organization should contain at least one App, with which any user can generate the credentials required to use the Token APIs.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603



Jorge Fernandez

@xurxo

Logout

Privacy Policy · Terms of Service

Welcome, Jorge Fernandez

Here you can manage your information, privacy and security for your Token Account

Account & Profile

You account settings and profile

Security

Settings and recommendations to help you keep your account secure

Notifications settings

Manage your push and email notifications preferences

Organizations

Create or edit an existing organization

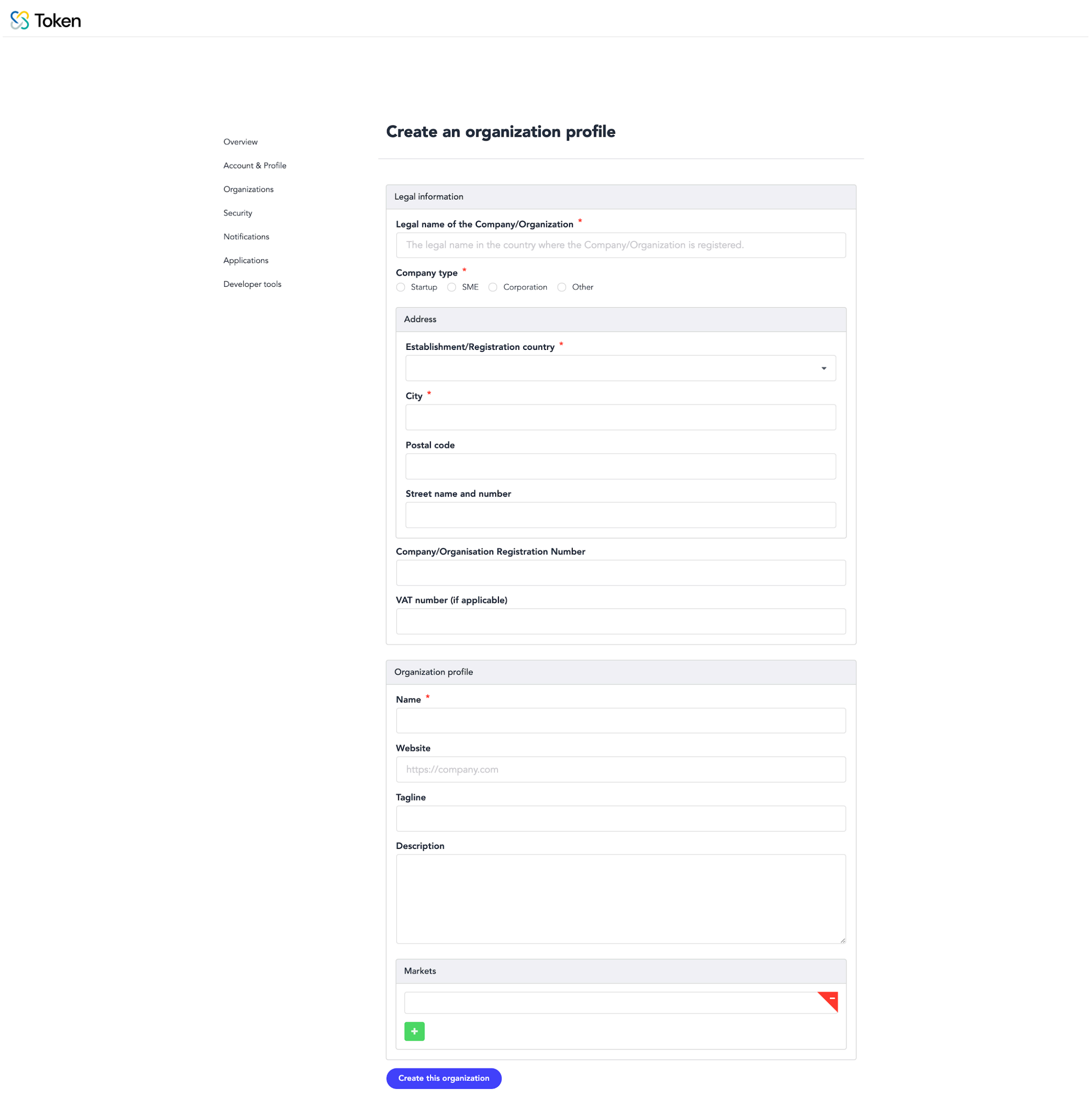
Applications

Manage your apps

Tools

Tools for developers

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603


Token

Create an organization profile

Legal information

Legal name of the Company/Organization *

The legal name in the country where the Company/Organization is registered.

Company type *

Startup SME Corporation Other

Address

Establishment/Registration country *

City *

Postal code

Street name and number

Company/Organisation Registration Number

VAT number (if applicable)

Organization profile

Name *

Website

https://company.com

Tagline

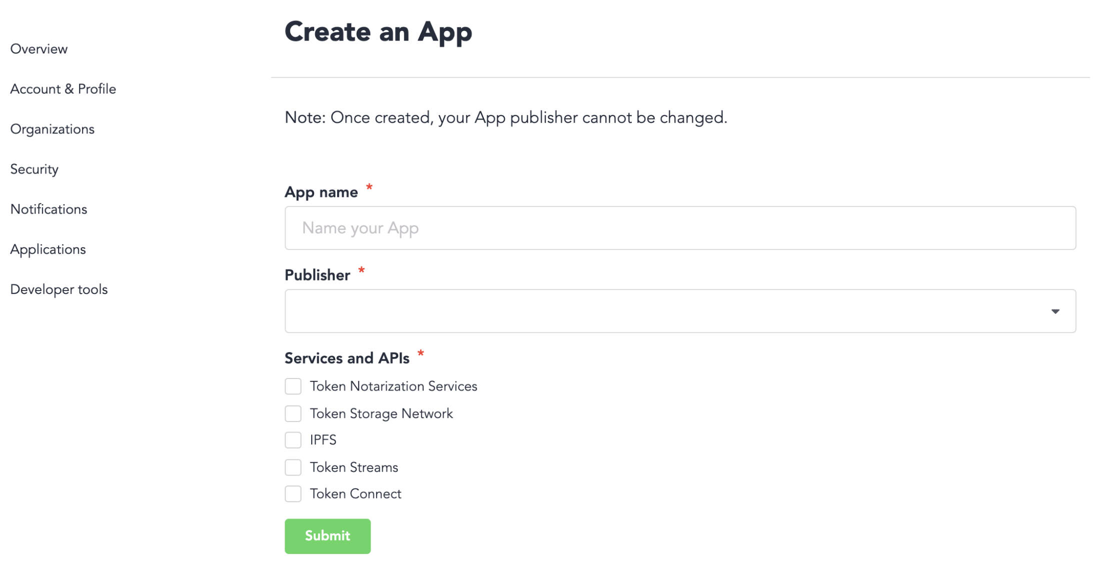
Description

Markets

Step 3. Create an application profile by creating an APP linked to an existing organization.

The App is where you can generate an APP ID and API secret key to start using the Token APIs.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603



Overview
Account & Profile
Organizations
Security
Notifications
Applications
Developer tools

Create an App

Note: Once created, your App publisher cannot be changed.

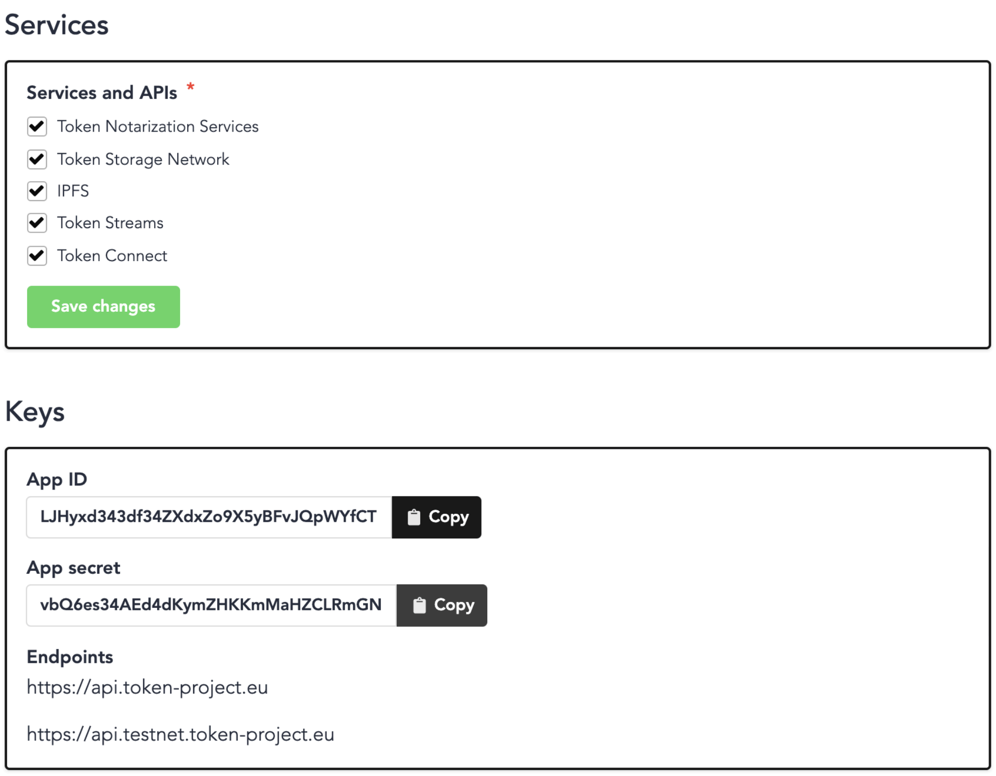
App name *
Name your App

Publisher *

Services and APIs *
- [ ] Token Notarization Services
- [ ] Token Storage Network
- [ ] IPFS
- [ ] Token Streams
- [ ] Token Connect

Submit

Step 4. Select the services your App wants to have access to. This generates a set of credentials to use the APIs.



Services

Services and APIs *
- [x] Token Notarization Services
- [x] Token Storage Network
- [x] IPFS
- [x] Token Streams
- [x] Token Connect

Save changes

Keys

App ID
LJHyxd343df34ZXdxZo9X5yBFvJQpWYfCT Copy

App secret
vbQ6es34AEd4dKymZHKKmMaHZCLRmGN Copy

Endpoints
https://api.token-project.eu

https://api.testnet.token-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

After having had correctly finalised all the above steps, the services are ready to be used.

The Token Platform allows any APP in development mode to use the APIs without restrictions and authentication of the API calls using just a combination of AppId + AppSecret. To move an APP to production mode additional steps are required, i.e. Deploying some nodes to the network, generating certificates or DIDs to identify the APP.

In the Developer Portal, there is documentation on each of the services and some code examples. The documentation provides information on the Rest APIs and how to get started. In the future, there will also be existing examples, with existing repositories, however, this will not be available in the first release.

Conclusion

The Token testbed is the first tangible step to make the Token Services available. Initially just available to the project partners it aims to provide a testing environment where the partners can start to get familiar with the decentralised and distributed technologies that will be provided by the project. It's intended that all partners involved in the PUCs and specially the technical partners create an account and start testing with the services. The documentation, complemented with workshops that are being provided should help the partners to better understand the services and to start testing and exploring them.

The sustainability beyond the project end of the test environment as such will be explored and decided by the partners analysing aspects related to how much is needed by the partners and potential early adopters and what are related financial implications.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

Annex - Token Services Description

In this Annex you can find a more detailed description of the initial services provided by the Token Platform. This is a non exhaustive list as some other services are under analysis. As previously stated just some of the services will be available in the testbed at this stage. Those are the ones related to blockchain notarization and to decentralised and distributed storage. For January of 2021 it is expected that all 4 the services (see their description below) with their different components will be available at production level. A decision at Token consortium level will be taken to decide if it makes sense to have the different services available in the testbed or directly at production level. This decision is also based on the economics aspect as to host the testbed and production networks may imply high costs of maintenance.

The services provided by the TOKEN platform are grouped on 4+1 blocks:

- Blockchain-based Notarization services
- Decentralised and Self Sovereign identity
- Decentralised and Distributed Storage
- Events and Messaging Streaming

1. Blockchain based Notarization Services

The Blockchain based notarisation services are intended to provide immutability and transparency to the services created using them. It is a service to prove that a transaction has taken place and allows them to be time stamped or even to include certain non-binary data in the record.

- **Timestamping**
  Token TTS (Trusted Time Stamping): A REST-API to provide anonymous, tamper proof time stamps for any digital content as a for Proof of Existence of a given document, data or transaction in a given time.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

- **Token Registry**
  A REST-API to provide tamper-resistant, immutable On-Chain storage.
- **Token Sign**
  A decentralized App providing document signing and verification using DIDs and blockchain to store the signatures/transactions. Token Sign will not be provided in the first release but in a later version of the platform.
- **Fiware Canis Major**
  Blockchain Adaptor: enabling the integration of the Context Broker.

This service is provided together with two Notarization APIs:

STAMP API: that allows you to create a hash of the data you want to anchor to the blockchain. Only the hash of the data will be stored on the blockchain.

ANCHORING API: This API allows you to hash your data and store additional non-binary data on the blockchain also. A hash can be created from a while or from a sting. For GDPR reasons, personal data should never be stored on the blockchain.

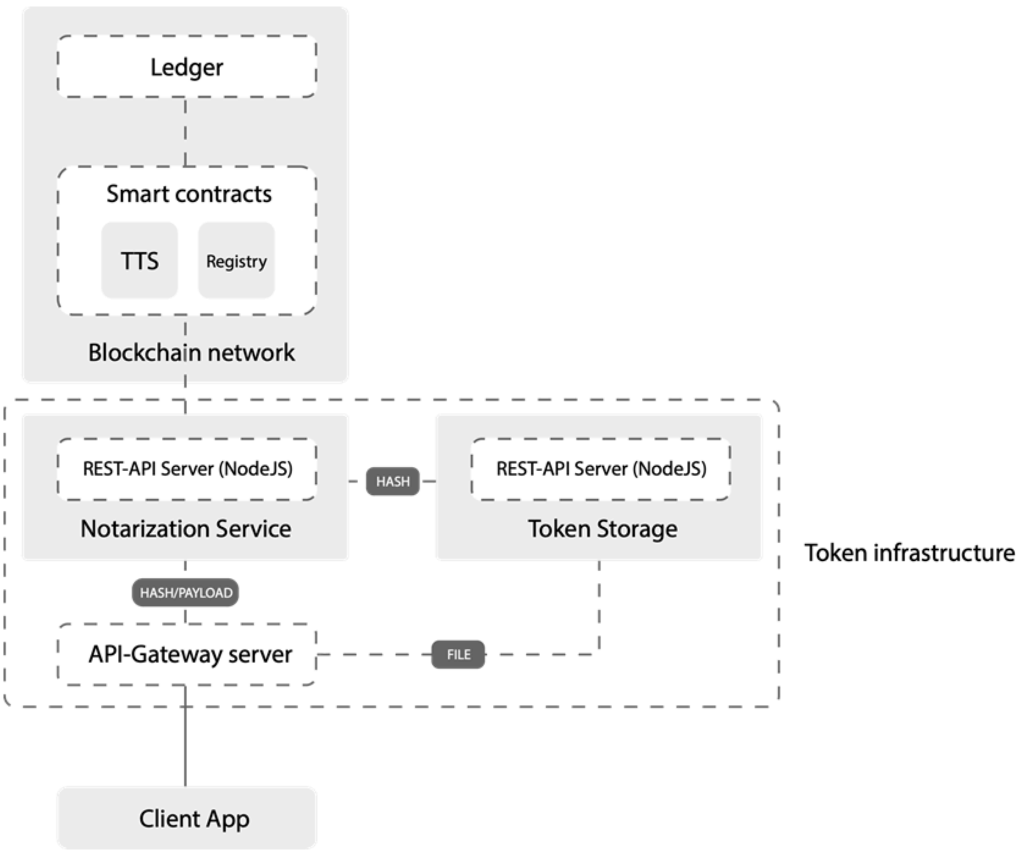
1.1. Components and Architecture

The following are the components of Blockchain based notarization.The Notarization services on the testbed are running on Chaincode with Hyperledger Fabric, however, the plan for 2021 is to also have a version compatible with Ethereum. In addition, it is possible to request the code and deploy on your own network (Fabric and Ethereum).

Main components of the service:

- Smart-contracts deployed to a Blockchain Network (Fabric/Ethereum based).
- A Rest API.
- API Gateway for pre-processing + Authentication/Authorization.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603



1.2. Use case- Notarizing Files and Non-Binary Data

Files: The API provides three methods of notarizing files:

a) Notarize a file by uploading it to the Token storage. The service calculates the SHA-256 hash value of the file contents, creates the file's notarization certificate that contains the information about the notarization status, and then queues the hash value for writing it to the blockchain. The file is stored in the token storage and can be easily accessed.

b) Notarize a file by sending it to the service. The file cannot be larger than 1 GiB. The logic is very similar to the method above, with the following exceptions: The file is not uploaded and stored in the token storage.

c) Notarize a file by sending a pre-calculated hash value of its contents to the notary service.

Non Binary Data:

a) Sending the payload to the API
b) Sending a pre-calculated hash to the API (TTS)

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

2. Decentralized and Self Sovereign Identity

2.1. Token Connect

Token Connect is an Identity Wallet implementing the DID AuthN profile for OpenID Connect. It provides the following functionality:

- Allows the user to login in a service with their Decentralized identifier.
- Allows Relaying Parties to use the Self Issued OpenId Protocol to authenticate the user.

Instead of an enterprise providing an Identity on behalf of a user, the user becomes the identity claim provider. This means, the user will not share his/her personal information with any external party. Hence, the user could decide what information will be shared with whom and when.

This component will facilitate through a restful API that the different components can make requests to a unique API answering the requests for the different services with the goal to simplify the process.

The first release will be compatible with did:ethr: method and any other method based on the same specification like did:jolo did:uport and any other method that allows the user the control of their own privateKey.

At this stage, it is intended only for authentication purposes. Therefore it does not provide the mechanisms to interact with verified credentials. Future releases may include support for verified credentials, sign documents and receive notifications.

2.1.1. Components

- No infrastructure involved. The User needs to install an identity wallet browser extension.
- The Relying Party needs to implement a library in order to interact with the user identity wallet.

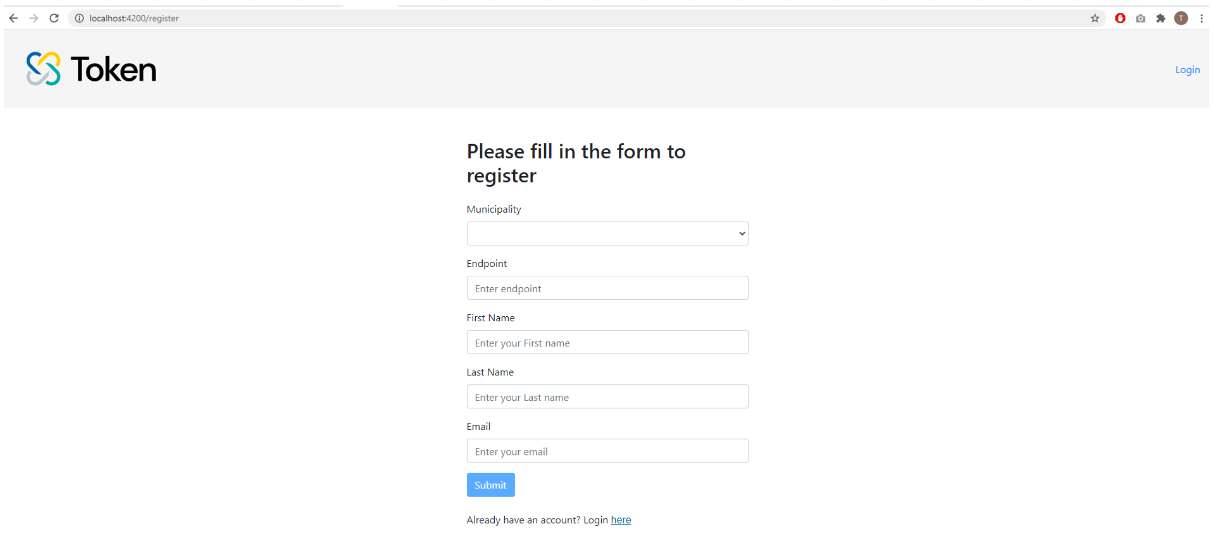
2.2. Self Sovereign Identity Solution

TOKEN''s CERTH SSI implementation is a platform in which a user can register, get a DID and request credentials. The user can have their credentials stored in their

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

wallet and access them quickly and easily, without downloading any special software. Thus, CERTH's SSI is functioning as a service (SSIaS). This solution removes the burden of e-government bodies to maintain their own servers, storage or even custom software as all these functionalities are provided out of the box. In this direction, any organization, agency, municipality and governmental service in general can take advantage of the unique characteristics of SSI at no cost and at no time!

- Registration:



Please fill in the form to register

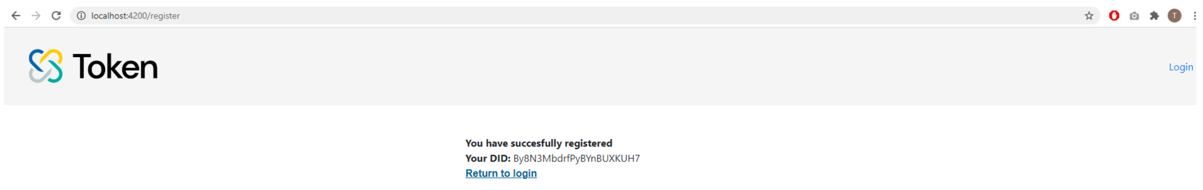
Municipality	
Endpoint	Enter endpoint
First Name	Enter your First name
Last Name	Enter your Last name
Email	Enter your email

Submit

Already have an account? Login here

When a user registers, the Endorser Agent creates a DID and makes a connection with the Trustee Agent. When the connection is established, the Endorser Agent sends a proposal to the Trustee Agent in order to issue an ID Verifiable Credential. Then, the Trustee Agent issues an ID credential to the Endorser Agent. Now the user has a DID and an ID Credential in her/his/its wallet.

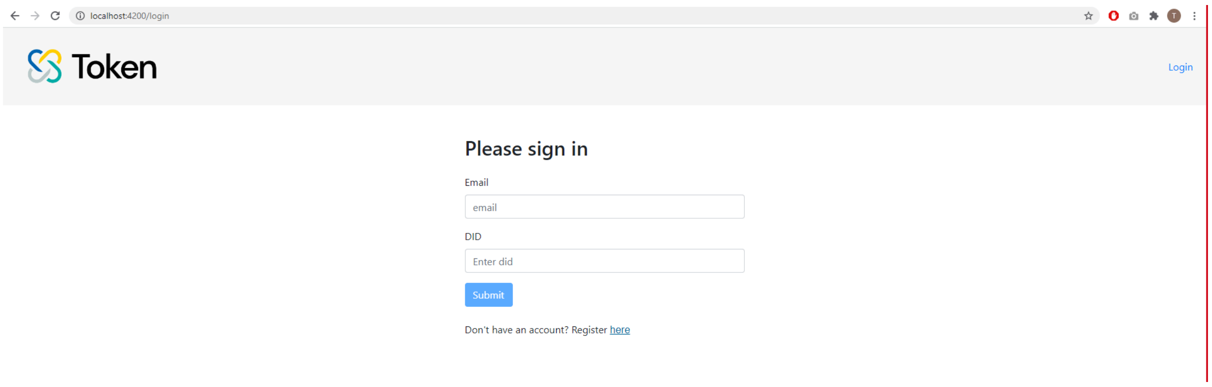
When the registration is completed, the user will be directed to a page that shows their DID. The user must keep somewhere safe this DID as a digital or hard copy, because it is their globally unique identifier and it is required in order to log in and communicate with any other service.



You have succesfully registered
Your DID: By8N3MbdrfPyBYnBUXKUH7
Return to login

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

- Log in:


localhost:4200/login

Token

Login

Please sign in

Email

email

DID

Enter did

Submit

Don't have an account? Register here

The user, after registers successfully, can log in to the platform with the DID that was created from the registration process.

The above transactions of the agents are held in corresponding PostgreSQL databases, one for each agent. They are also stored along with other important metadata information of the user in a MySQL database.

3. Decentralized and Distributed Storage

3.1. Token Storage Network

If you've used cloud storage before, you'll find token storage easy to understand. Unlike traditional cloud services, the service is built on open, decentralized protocols including the IPFS and Libp2p. You can serve websites, data, and even apps using the storage network.

The Storage Network and APIs are packed with useful features, including:

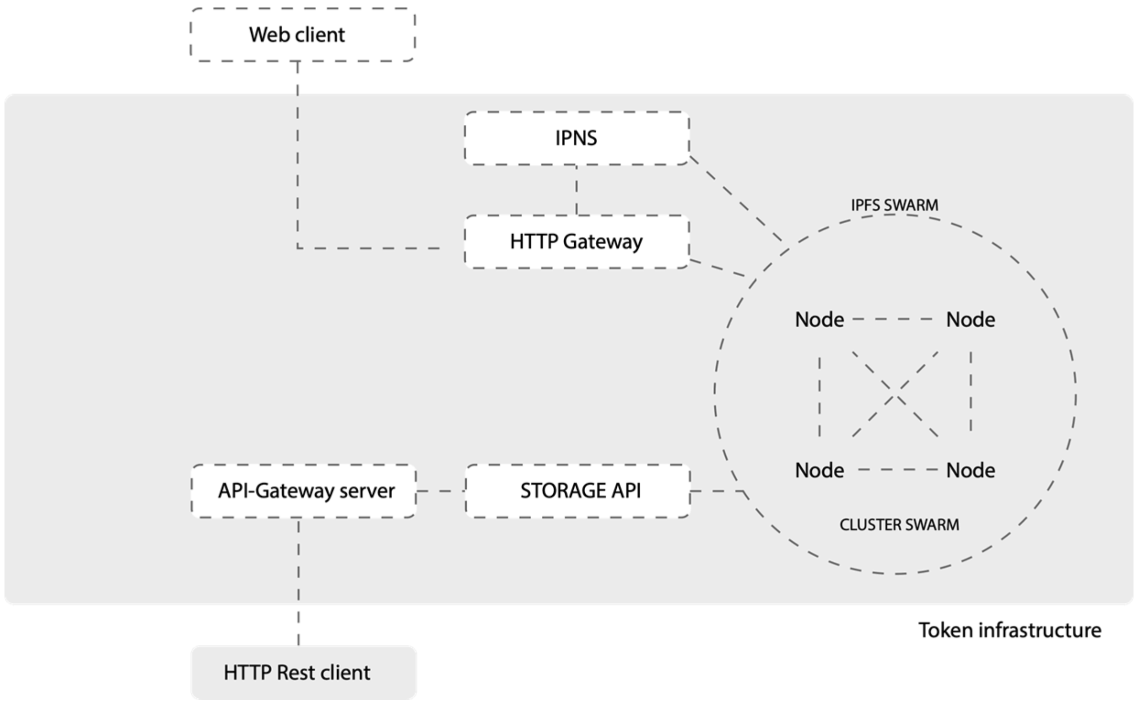
- Create public/private (encrypted) datastores where apps can store data
- (Soon) Create personal datastores where app users can store data
- Use public datastores to distribute content and apps to the web.
- Collaboratively manage Datastores as an app/organization
- Create automations with other Token Services (Files notarization, Send notifications with attachments, attach files to batch processing pipelines, etc.)

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3.1.1. Components and Architecture

The following are the components of the TSN:

- IPFS cluster
- IPNS
- HTTP Gateway
- HTTP REST API to manage documents/datastores
- API Gateway for pre-processing + Authentication/Authorization
- Token services connectors (Notarization, Stream processors, DID resolver/cache, encrypting).



3.1.2. Use Case

When we combine Blockchain and TSN, we gain the ability to timestamp any data we want, no matter how big the size.

Let's say that a company signed a rather large legal agreement. The signed PDF of that agreement was stored on TSN and the corresponding hash was stored onto a blockchain.
Now, let's say there was a dispute where one party claimed the agreement had never been signed. This could easily be disproved by referencing the block where the hash of the agreement was added to the blockchain and since the hash was added to the blockchain at the time of upload to the TSN network, the signed document was timestamped in a tamper proof way. And, because TSN provides tamper-proof content

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

retrieval, it can be proven that the content the hash points to has not been altered in any way.

3.2. Token Public IPFS Services

3.2.1. IPFS Web Gateway

Token's read-only IPFS Web Gateway acts as a bridge between traditional web browsers and InterPlanetary File System (IPFS).

Through the gateway, Internet users can browse files and websites stored by third parties on the IPFS public network quickly and easily, without downloading any special software, as if they were stored in a traditional web server.

More information on the IPFS Web Gateway can be found here

3.2.2. IPFS Storage & Pinning service

Token's IPFS Storage & Pinning service simplifies decentralized storage offering redundant and persistent data storage on the IPFS public network.

Through the Token's IPFS Storage API users can upload, store & fetch files from the IPFS public network in an easy to use and performant way, while it built in pinning orchestration service ensures all uploaded information is replicated across multiple nodes and retained and accessible as long as needed.

We hope that our IPFS services will serve as the platform for highly-reliable and security-enhanced web applications.

More information on the IPFS Storage & Pinning Service can be found here

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

4. Messaging and Events Streaming (Token Streams)

The objective of Token Stream is to communicates securely and reliably with end-to-end encrypted messaging from App2App-App2User-User2User

The WebSocket Streams API provides mechanisms for sending and receiving messages between users using DIDs or PKI where users hold private keys linked to their identity. With just their private and public key, a user can send and receive encrypted messages to other users in an app.

Combined with the Notarization services it will also provide evidence relating to the handling of the transmitted data, including proof of sending and receiving the data.

Other use cases

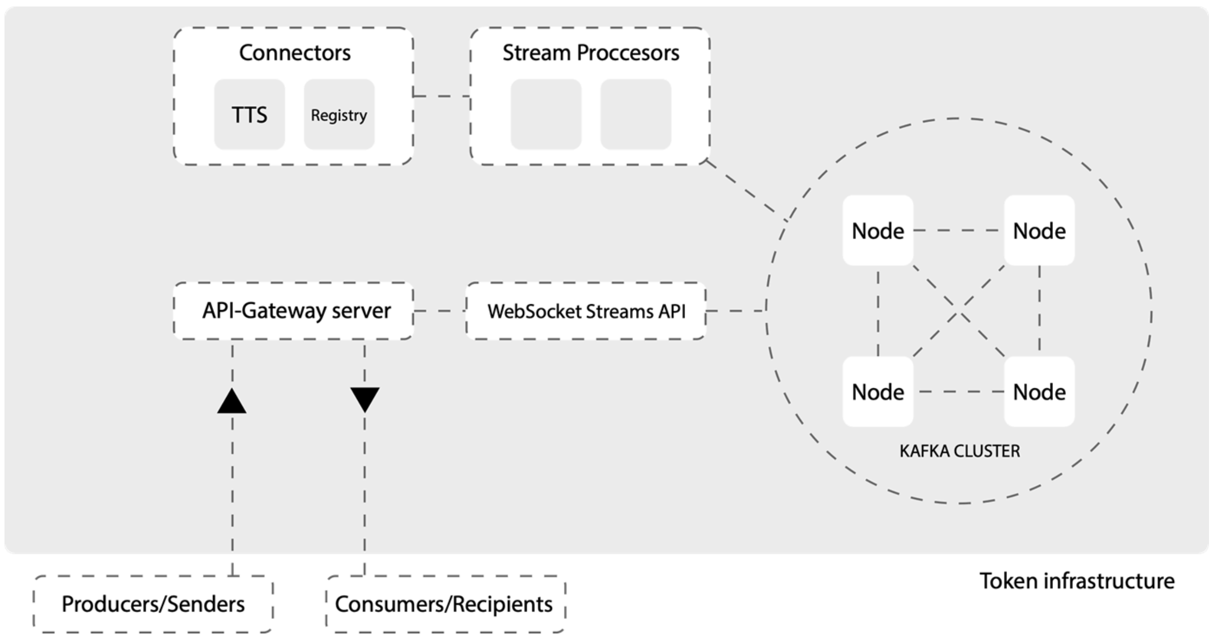
- Data pipelining
- Orchestration
- Chat
- Batch job scheduling

4.1. Token Streams Components and Architecture

The following are the components of Token Streams:

- Kafka cluster
- Token services connectors (Notarization, DID resolver/cache)
- Preconfigured - Token Stream processors (ERDS)
- WebSockets API to produce/consume messages/streams
- API Gateway for pre-processing + Authentication/Authorization

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603



4.2. Token Streams Use Case (ERDS)

Steps:

- The sender app connects to the Websocket API
- The sender connects to a specific topic
- The sender sends the request to send a message.
- This includes the message and the recipient DID or Public Key
- The Service resolves the DID and gets the DID public key
- The service encrypts the message with the recipient public key and add it to the queue
- The recipient connects to the WEBSocket API and its own Topic/channel
- Receives the message, decrypts it with its private key
- The Notarization connector may store all the related transactions to the blockchain (sent, queued, received, open)

This project has received funding from the European Union’s Horizon 2020 research and innovation program under Grant Agreement No 870603