Weldentity Documentation

Junqi Zhang

Aug 04, 2020

Contents:

Weldentity™

CHAPTER 1

What is WeIdentity?

WeIdentity is a blockchain solution on Open Consortium Chain to serve as a hub for identity authentication by establishing identity of entities (e.g. persons or objects) on the chain and allowing the interchange of such information among organizations when authorized. WeIdentity is an open source platform built by WeBank and promotes the values of Open Consortium Chain: streamline resources, collaborate to produce values and serve the public.

1.1 Modules

WeIdentity includes two major modules: WeIdentity DID and WeIdentity Credential.

1.1.1 Decentralized Identifiers (WeIdentity DID)

Traditionally, user identity is issued and managed by single centralized organization. With the advent of blockchain technology, it is possible to publish and distribute user identity on chain to allow more than one organization to manage on as a multi-centers solution WeIdentity DID Module has come with a distributed identification protocol based on FISCO-BCOS Blockchain Platform, and W3C DID specification, to create identities on chain and associate it with any person or object in the real world. Moreover, DID ensures the Entity with full rights of control and ownership of the identities.

The design goals of WeIdentity DID:

1.1.2 WeIdentity Credential

There are a lot of credentials describing identity in daily life such as personal identity card, driving license, account book, prescription, graduate certificate, property ownership certificate and credit report. WeIdentity Credential offers a complete set of W3C Verifiable Credentials based solutions designated to standardize and digitize such credentials into a verifiable and interchangeable format. The solution also supports Selectively Disclosure of Credential attributes and generating evidence of Credentials on blockchain.

WeIdentity encourages certificate organization to issue their own standardized credential templates to enrich the ecosystem on open consortium chain.

1.1.3 More

- Use Cases and Scenarios (Chinese Version)
- WeIdentity Specification (Chinese Version)
- FAQ

1.2 Current Status

WeIdentity is running on top of FISCO-BCOS with JAVA SDK provided for developers, please review the Installation & Deployment guide and SDK user guide listed below:

1.3 Diving in

Now, please feel free to dive in via this page for a one-stop experience of WeIdentity.

1.4 Contact Us

Email：weidentity@webank.com

1.4.1 What is WeIdentity?

WeIdentity is a blockchain solution on Open Consortium Chain to serve as a hub for identity authentication by establishing identity of entities (e.g. persons or objects) on the chain and allowing the interchange of such information among organizations when authorized. WeIdentity is an open source platform built by WeBank and promotes the values of Open Consortium Chain: streamline resources, collaborate to produce values and serve the public.

Modules

WeIdentity includes two major modules: WeIdentity DID and WeIdentity Credential.

Decentralized Identifiers (WeIdentity DID)

Traditionally, user identity is issued and managed by single centralized organization. With the advent of blockchain technology, it is possible to publish and distribute user identity on chain to allow more than one organization to manage on as a multi-centers solution WeIdentity DID Module has come with a distributed identification protocol based on FISCO-BCOS Blockchain Platform, and W3C DID specification, to create identities on chain and associate it with any person or object in the real world. Moreover, DID ensures the Entity with full rights of control and ownership of the identities.

The design goals of WeIdentity DID:

WeIdentity Credential

There are a lot of credentials describing identity in daily life such as personal identity card, driving license, account book, prescription, graduate certificate, property ownership certificate and credit report. WeIdentity Credential offers a complete set of W3C Verifiable Credentials based solutions designated to standardize and digitize such credentials into a verifiable and interchangeable format. The solution also supports Selectively Disclosure of Credential attributes and generating evidence of Credentials on blockchain.

WeIdentity encourages certificate organization to issue their own standardized credential templates to enrich the ecosystem on open consortium chain.

More

- Use Cases and Scenarios (Chinese Version)
- WeIdentity Specification (Chinese Version)
- FAQ

Current Status

WeIdentity is running on top of FISCO-BCOS with JAVA SDK provided for developers, please review the Installation & Deployment guide and SDK user guide listed below:

Diving in

Now, please feel free to dive in via this page for a one-stop experience of WeIdentity.

Contact Us

Email：weidentity@webank.com

1.4.2 Beginner's Guide

Installation Guide

This guide gives an instruction on installing and running WeIdentity in simple ways.

1. Prerequisites and Check List

- Please prepare a server with internet access. You may find more details from below check list.

Network Requirements:

- *Enable server to download related installation files from internet.*
- *Enable your browser to visit WeIdentity Web Tool GUI via http.*
- *Enable communication among WeIdentity and FISCO BCOS blockchain nodes.*

2. Installation

1) Install Dependencies

- Run below commands one by one to install Openssl,Curl,Git,Openjdk,Mysql,Sdkman and Gradle on the server.

```
sudo apt install -y openssl curl
sudo apt install -y git
sudo apt install -y default-jdk
sudo apt-get install mysql-server-5.7
sudo apt install -y unzip
sudo apt install -y zip
curl -s "https://get.sdkman.io" | bash
source "$HOME/.sdkman/bin/sdkman-init.sh"
sdk install gradle 6.4
```

- Run below commands to setup Mysql database.

```
sudo mysql -u root
```

```
create database weid;
GRANT ALL PRIVILEGES ON weid.* TO weid@"%" IDENTIFIED BY "weid@123";
exit;
```

- Run below commands to check if the depandencies have been installed successfully.

```
sdk version
java -version
gradle -v
sudo mysql -v
```

2) Install FISCO BCOS and Weldentity

- Run below command to install FISCO BCOS and FISCO BCOS Console.

```
cd ~ && mkdir -p fisco && cd fisco &&
curl -LO https://github.com/FISCO-BCOS/FISCO-BCOS/releases/download/v2.5.0/build_
↪chain.sh && chmod u+x build_chain.sh &&
bash build_chain.sh -l "127.0.0.1:4" -p 30300,20200,8545 -v 2.5.0 &&
bash nodes/127.0.0.1/start_all.sh &&
cd ~/fisco && curl -LO https://github.com/FISCO-BCOS/console/releases/download/v1.
↪0.9/download_console.sh && bash download_console.sh &&
cp -n console/conf/applicationContext-sample.xml console/conf/applicationContext.
↪xml &&
cp nodes/127.0.0.1/sdk/* console/conf/
```

- Run below commands one by one to check if FISCO BCOS has been installed successfully.

```
ps -ef | grep -v grep | grep fisco-bcos
tail -f ~/fisco/nodes/127.0.0.1/node0/log/log*  | grep connected
tail -f ~/fisco/nodes/127.0.0.1/node0/log/log*  | grep +++
```

- Run below command to install WeIdentity Web Tool.

```
cd ~ && mkdir -p weid && cd weid &&
sudo apt install git &&
wget -c https://github.com/WeBankFinTech/weid-build-tools/raw/master/common/script/
↪install/weid-install.sh &&
```

(continues on next page)

(continued from previous page)

```
chmod u+x weid-install.sh &&
cd ~/weid && ./weid-install.sh -t en &&
cd weid-build-tools &&
./start.sh
```

There are two ways to deploy WeIdentity JAVA SDK and WeIdentity Contracts.

- (Option 1) Use command line to deploy.
- Update configurations in `~/weid/weid-build-tools/run.config` as below.

```
blockchain_address=127.0.0.1:20200
blockchain_fiscobcos_version=2
org_id=demo
chain_id=1
group_id=1
mysql_address=127.0.0.1:3306
mysql_database=weid
mysql_username=weid
mysql_password=weid@123
cns_profile_active=test
```

- Copy FISO BCOS blockchain key files

```
cd ~/weid/weid-build-tools &&
cp -f ~/fisco/nodes/127.0.0.1/sdk/ca.crt ~/weid/weid-build-tools/resources &&
cp -f ~/fisco/nodes/127.0.0.1/sdk/node.crt ~/weid/weid-build-tools/resources &&
cp -f ~/fisco/nodes/127.0.0.1/sdk/node.key ~/weid/weid-build-tools/resources
```

- Deploy WeIdentity JAVA SDK and WeIdentity Contract.

```
cd ~/weid/weid-build-tools &&
chmod +x compile.sh &&
./compile.sh &&
chmod +x deploy.sh &&
./deploy.sh
```

The output should be similar to below.

```
contract is deployed with success.
=========================================.
weid contract address is 0x4ba81103afbd5fc203db14322c3a48cd1abb7770
cpt contract address is 0xb1f3f13f772f3fc04b27ad8c377def5bc0c94200
authority issuer contract address is 0xabb97b3042d0f50b87eef3c49ffc8447560faf76
evidence contract address is 0x8cc0de880394cbde18ca17f6ce2cf7af5c51891e
specificIssuer contract address is 0xca5fe4a67da7e25a24d76d24efbf955c475ab9ca
=========================================.
```

- (Option 2) Use WeIdentity Web Tool for deployment (in Chinese language).
- Open URL `http://{public ip of the server}:6102/guide.html` via browser and follow the guide shown on the web page. (You may copy the values from Option 1)

```
http://127.0.0.1:6102/guide.html
```

- Choose a role “As a Committee Member”(recommended) or “As a non Committee Member”.
- Setup FISCO BCOS.
- Define main group id.
- Setup Mysql (Optional).
- Click button to generate admin account.

- Click button to deploy WeIdentity Contracts and WeIdentity JAVA SDK as a Committee Member only.

1.4.3 FAQ

- **What can the user do on his/her/its data?**

1. User (a person, an object or an organization) has full control and ownership of the digital identifier without reliance on external authorities.
2. User's digital identifier can be portable to other systems and be used as long as the identifiers support DIDs and DID methods.
3. Users can authorize the access of their data to a third party.
4. User can decide what information from digital credential should be disclosed whereas the validity and the authenticity of the data can still be preserved.

- **Which organizations or agencies should be involved in KYC (Know your client) under WeIdentity?**

It is all down to the nature of business on which organizations should be involved in KYC. In other words, WeIdentity will never interfere in the existing KYC process. Nor it has any obligations of/influences over involving any organizations in the KYC process.

- **What kind of credentials are supported by WeIdentity? What kind of organizations this credential is associated with?**

WeIdentity can restructure and transform paper credentials to digital forms in two categories.

1. Authoritative credential: A WeIdentity credential which is digitally signed by an issuing authority or organization. For example, identity card, driving license, passport, academic certificate and medical prescription.
2. Customized credential: A WeIdentity credential which is digitally signed by a person. For example: authorization certificate, promissory note and invitation.

- **How to apply WeIdentity in a business context like digital escrow, supply chain, trading, and gaming?**

WeIdentity can be applied in all business contexts where proof of one's identity, access of authorized information or exchange of data are required. However, different business scenarios with different requirements will derive specific adoptions of the technical solution.

- **How to obtain the detailed information which is stored off-chain?**

WeIdentity never publishes private information on chain and such will only be stored separately off-chain. There are two ways in retrieving these information:

1. User can first download the information through User agent, then submit the information online or via QR code to the party who needs to access the information.
2. On the contrary, the user can authorize User Agent to access the data directly, if there is a data transfer channel already built between User Agent and data consumer.

- **How to register a new user or organization onboard to the chain?**

New user must go through User Agent to access the chain. And new organizations are advised to register while taking their roles and business scenarios into account:

1. In most business models, the transaction initiator normally plays the role of blockchain operator, who is expected to deploy all nodes for the consortium chain and provide an open platform solution for other business players to connect.
2. Other business players can either deploy their own nodes with permission from the initiator, or join the consortium blockchain through the open platform provided.

- **How can WeIdentity ensure the authoritativeness of information provided by the issuing organization, e.g. making sure a sustainable and stable provision of reliable data from genuine source?**

In a WeIdentity project, data credibility is built upon the trust and recognition people have on the data provider as an authority. It is down to the capability of the data provider (e.g. government) to maintain its authority of information and quality of data service.

- **Which organizations can participate in consensus decision and what are the requirements?**

Parties like data provider, data consumer and User Agent could be eligible to take part in consensus process, but such could vary with and depend on the nature of business or the role an organization takes.

- **How to migrate the data of WeIdentity DID to other platform ?**

1. WeIdentity SDK provides interface for exporting data (e.g. for user agent's use when data migration requires) of WeIdentity Document into JSON file format.
2. WeIdentity SDK also provides interface for importing WeID Document from other WeID platforms. Once imported, the WeIdentity Document will be created with same attributes as origin.

- **How to migrate the data of Credential to other platform?**

In WeIdentity, Credential is implemented following the specification of W3C verifiable credentials and such can be stored or managed by different organizations in different use cases. WeIdentity standardizes the function interface to allow the organization to import data to or export data from the platform with user's permission.

- **Does WeIdentity provide batch processing interface?**

Currently batch processing is not yet ready, however it will be provided in a later release.

- **What is the difference between WeIdentity DID and Standard DID ?**

WeIdentity DID has further implemented a distributed and multi-centered identity authentication protocol (WeIdentity is required to be run on a distributed ledger platform) based on W3C DID specification to allow a person or an object to be registered, identified and authenticated on chain.

- **What is CPT and how CPT is used?**

CPT (Claim Protocol Type) is a data structure which can be customized and used as a template to describe a type of Credential such as driving license and academic certificate, therefore each Credential must define its CPT. For instance, employer can define a CPT and then register it on WeIdentity blockchain to describe the data structure of the employee access card to manage the access control within the company.

- **When a data consumer fetches user data from data provider, how to ensure the process is authorized?**

When Party A (data consumer) wants an access to User X's data (data owner) from Party B (data provider), Party A must first receive an "Authorization Credential"(in CPT101 or customized CPT) from User X.

Once received, Party A then submits a data access request to Party B with User X's "Authorization Credential" as an attachment through data transfer interface. After Party B receives and verifies the "Authorization Credential", Party B then returns the requested data to Party A.

- **What to do when an issuer/a person loses a private key?**

Once the private key is lost, the 'Recovery' mechanism can help to reset the public key of authentication at WeIdentity. However it requires the owner of WeIdentity DID having assigned a user for key recovery upfront. In the future, WeIdentity will support multiple recovery users. Any user, or a required number of users on the delegate list can reset the key.

- **How to re-issue or revoke an issued Credential?**

WeIdentity Credential allows organizational or individual issuers to revoke issued Credentials when needed. To re-issue the Credential, WeIdentity will treat it as a new Credential with a new Credential ID. At the same time, WeIdentity allows issuer to renew or extend the expirity date of a Credential.

- **Can Credential be forged? Any way to prevent the forgery?**

WeIdentity Credential currently adopts ECDSA signature algorithm, and will support RSA signature in future releases. The effort to forge a Credential is the same as to compromise an ECDSA/RSA private key with a given key-length, which makes forgery practically impossible if the private key of Credential is securely kept.
