# Research on decentralized identity and access management model based on the OIDC protocol

Kunying Li*, An Ren, Yu Ding, Ying Shi, Xiaobo Wang
Computer Application Technology Department,
PetroChina Research Institute of Petroleum Exploration & Development,
Beijing 100083, China
* Corresponding author: likunying@petrochina.com.cn

***Abstract*—In the increasingly diverse information age, various kinds of personal information security problems continue to break out. According to the idea of combination of identity authentication and encryption services, this paper proposes a personal identity access management model based on the OIDC protocol. The model will integrate the existing personal security information and build a set of decentralized identity authentication and access management application cluster. The advantage of this model is to issue a set of authentication rules, so that all users can complete the authentication of identity access of all application systems in the same environment at a lower cost, and can well compatible and expand more categories of identity information. Therefore, this method not only reduces the number of user accounts, but also provides a unified and reliable authentication service for each application system.**

***Keywords-OIDC protocol，Decentralized ID，Certificate Authority***

## I. Introduction

In today's open network environment, when users log in to different application systems to obtain business information, they need to input identity authentication information to the system, which brings great inconvenience to users. Therefore, the construction of a set of certification system suitable for all systems is particularly important for the growing information system cluster. In the decentralized system, anyone is a node, and anyone can be a center. Any center is not permanent, but phased, and no center is mandatory for nodes [1]. This paper compares and analyzes the main schemes at home and abroad, focusing on the identity management scheme based on blockchain represented by shocard, uport and civic, and analyzes its outstanding features and impact on other schemes [2]. A new scheme of identity authentication technology based on blockchain application mode is proposed [3]. By using the tamper ability of blockchain protected storage information, distributed storage, information maintenance, security transmission, establishment of distributed mutual trust relationship and identity security verification can be realized. It also studies the DID plan of Microsoft, NDB plan of Australia, GDPR of EU and network security requirements of New York State financial service company, which have clear plans and requirements for decentralized personal identity management scheme [4]. With the continuous promotion of information construction, the so-called unified identity authentication service has been implemented in a specific field. When users log in to a system that does not belong to the scope of the unified service, they often face the problem of re docking and development. Therefore, according to the idea of distributed authentication service of blockchain, we propose a set of decentralized identity authentication access management system designed by OIDC technology, so as to solve the head problem caused by centralized authentication.

## II. Basic concept of decentralized identity authentication

Decentralized identity authentication generally means that each application system accessed is like an independent shopping mall. Users use these applications like shopping malls. Shopping malls use membership cards to identify users. Then we generate a special membership card for users based on their information. Each membership card can be used by all shops in the corresponding shopping mall. At the same time, after two large-scale shopping malls pass mutual authentication and authorization, users also have the membership rights of these two shopping malls. This is a safe way of authorization. If you don't have this membership card and directly expose your personal information, it's equivalent to going shopping with your ID card. It's far safer to lose a membership card number than to lose one.

### *A. Solve data privacy security problems*

In the example mentioned above, the shopping mall records the user's membership information to generate a membership card, and then the merchant identifies the user by reading the membership card. if the user directly uses the account and password to log in for many times, then the user data may be trafficked at will in the process of platform flow. Therefore, the decentralized idea is to use the zero-knowledge proof that there is no real information about the user when making the user authentication token. Thus, it can realize multi-link trusted data exchange and access after verification, so that the privacy information is no longer circulated in the business link, so the risk of theft is greatly reduced.

### *B. Get through the value of data utilization in all links*

For users, it is very inconvenient to repeatedly register personal information, and users can't control this information after outputting this information. In the decentralized authentication service, users have the ownership of user data

978-1-7281-5902-7/20/$31.00 ©2020 IEEE
DOI 10.1109/ECIT50008.2020.00065

generated in each platform, which can realize real-time authorization or recovery. Finally, we can make use of decentralized digital identity to let users hold this part of data and get the return of data being used, so as to realize the value of user data utilization in all links.

### *C. Reduce the cost of user authentication*

In the daily development of the system, it is difficult for the project builder to authenticate the user's identity, and the high cost has always been a common problem. Then this method of this paper will help users to solve the problem of "how to prove that I am me". Nodes in the same environment only need to apply for validation, and users can give validation. This can reduce the cost and efficiency of identity authentication for users and business parties.

### *D. More convenient maintenance service*

The decentralized mode of thinking does not mean that there is no central node, but that each node can be used as a service point for authentication, so for the user's identity authorization record, it can easily open the third-party authoritative nodes, such as the enterprise strategic business system, personnel management system and the existing unified identity authentication management system. In this way, user data can be maintained and called more easily.

## III. DECENTRALIZED IDENTITY DESIGN

Decentralized identifier (DID) is a new type of identifier with global uniqueness, high availability, resolvability and encryption verifiability [5]. This standard is applicable to all applications under the same domain model. The main purpose of this standard is to solve the problem of non-standard and noncredit between various systems, to solve the identity non interworking and users really have their own unclassified identity authentication rights.

In this study, referring to the design of DID for user identity identifier, the identifier is divided into basic information and verifiable declaration part. As shown in Table 1, the designed ID token identification token contains the user's non secret information.

TABLE I BASIC INFORMATION OF USER IDENTITY

| *NO* | *Parameter name* | *Description content* |
|---|---|---|
| 1 | Issuer Identifier | Provide the unique identification of the certification information provider. Generally, it is an HTTPS URL |
| 2 | Subject Identifier | The identification of EU provided by ISS is unique within the scope of ISS. It will be used by clients to identify unique users. |
| 3 | Audience | Identifies the audience for the ID token. client_id of oauth2 must be included. |
| 4 | Expiration time | Expiration time. ID token beyond this time will be invalidated and will no longer be verified. |
| 5 | Issued At Time | Specific issuing time of this identity |
| 6 | Authentication Time | EU certification time |
| 7 | nonce | The random string provided by the RP when sending the request is used to slow down replay attacks. It can also be used to associate the session information of ID token and RP itself. |

All the above parameter information as the basic ID token of user identity is valid for all systems using the system authentication service. This is a security token, and users can have access to other application systems at any time during the validity period， The verifiable statement is regarded as a higher level of system level security authentication, which is the value of establishing a secure access system [6]. The verifiable declaration part grants specific issuing verification information, which records the user's operation information, including identifier registration authority, which system to log in from, whether the logged in system has special verification channel, configured verification return address, etc. It can be seen from this that even if the underlying token is stolen but there is no verifiable declaration as the background of the security access token, it cannot be successfully verified.

## IV. THE IMPLEMENTATION OF IDENTITY MANAGEMENT MODEL BASED ON THE AUTHENTICATION MECHANISM OF OIDC

Based on the idea of identity token designed above, a new authentication mechanism, OIDC identity authorization protocol is used, which is a new generation of authentication and authorization protocol based on the integration of [7] OAuth2.0 and [8] OpenID. At present, it has been widely used and recognized all over the world. The decentralized idea is further implemented from text to solution, and other information such as user identity is obtained through the coordination verification of public key and private key. This mode avoids eavesdropping and interception from the perspective of data communication, so that the identity information can be completely closed-loop operated on the data source.

OIDC is the abbreviation of OpenID connect [9]. It builds an identity layer on the secure access communication authentication service model of oauth2.0, which can provide perfect identity authentication function. The protocol uses the authorization server of oauth2.0 as the entrance of identity authentication service of each application system, and transmits the corresponding identity authentication information to the client. More importantly, all the sub nodes can deploy corresponding IDPs, and then synchronize the user data through the unified standard data transmission specification, so that after any IDP loses the authorization, other IDPs can be accessed normally, which improves the robustness of the system. The specific application scenario is shown in Figure 1:

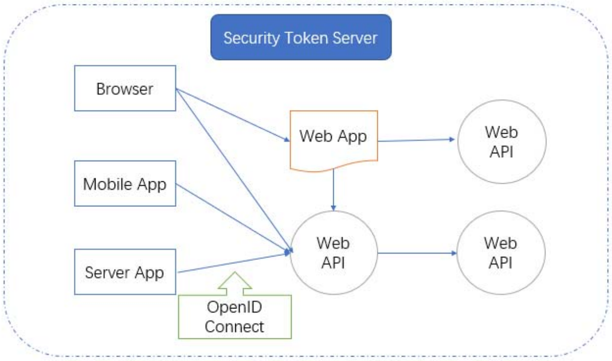
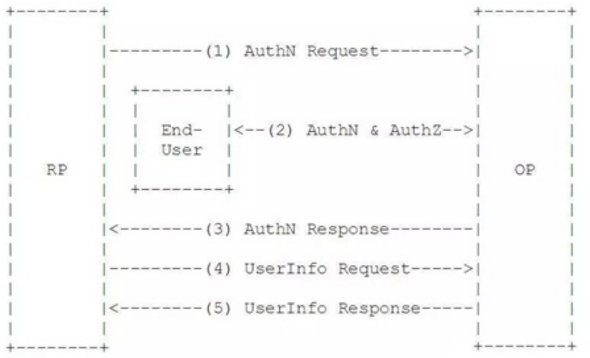


Figure 1. The process of OIDC

In the face of many business systems, in order to unify the fast reading security of all kinds of identity authentication interfaces, security token service is an API authentication and authorization solution implemented by using the OIDC protocol to solve this problem. The service encodes according to the previously defined identity token rules, generates the key and quickly exports the public key to the corresponding API authentication service interface. The encrypted string is used in the authentication communication between servers that users can't perceive. If the validity period is exceeded, the token will automatically fail, which not only facilitates users but also provides a deep level guarantee for data security.

From the perspective of data flow, IDP service provides a set of identity authentication rules for security encryption, through which users' information is encrypted to generate tokens, and then flows to various application systems. The application end does not send the authentication request directly to the server to obtain the required resources, but first sends the account authentication request through the authentication service. After the server authenticates the user's identity and the trusted statement, it will return an encrypted token string as the identity token, so the user can access all the credit system through the token at any time during the validity period. The specific process is shown in Figure 2:



```
+--------+                                   +--------+
|        |                                   |        |
|        |---------(1) AuthN Request-------->|        |
|        |                                   |        |
|        |  +--------+                       |        |
|        |  |        |                       |        |
|        |  |  End-  |<--(2) AuthN & AuthZ-->|        |
|        |  |  User  |                       |        |
|   RP   |  |        |                       |   OP   |
|        |  +--------+                       |        |
|        |                                   |        |
|        |<--------(3) AuthN Response--------|        |
|        |                                   |        |
|        |---------(4) UserInfo Request----->|        |
|        |                                   |        |
|        |<--------(5) UserInfo Response-----|        |
|        |                                   |        |
+--------+                                   +--------+
```

Figure 2. Authentication data interaction diagram

In the first step, an important statement definition is the scope parameter designed based on OpenID, which is also a difference from the traditional OAuth2 authorization. This parameter directly determines whether the entry can access the authorization area and access the IDP authentication service interface. Second, in the second step, end user is a resource protected by the protocol. After RP gets access token, it can request the service to obtain its related claims. In order to avoid too large user data, it can close some extended attributes and transfer some important unique identifiers as the main data stream. Therefore, for the whole architecture system itself, this protocol is a completely open standard, and supports many IDP holders. It is very simple to get through the whole identity authentication process. Only by transforming the existing system identity and authentication protocols into the OIDC model, we can realize the decentralization of way authentication. In this way, the security and reliability of the user's basic information are fundamentally solved, and the working efficiency of the whole link is improved.

## V. Application and Implementation

Compared with the traditional business system user authentication method, this research will apply the model based on the OIDC protocol in a large integrated platform. The authentication center is fully installed with the identity management model based on the OIDC authentication mechanism. The specific steps of data access are as follows:

1) Users log in to the application through the browser.

2) The application redirects to the platform OIDC server to return the Redirect URL to the browser. If the user is not logged in at this time, he or she will be returned to the login OIDC server.

3) Users log in to the platform OIDC service through a browser and request authorization numbers.

4) The platform OIDC service redirects to the application system and returns the authorization number to the browser.

5) Browsers use authorization numbers to request identity tokens from platform OIDC services.

6) Platform OIDC service authentication passes and returns to the browser an identity token that is encrypted and decrypted through OpenSSL. When the browser gets the identity token, it accesses the identity service to get the user's final personal information.

At present, through the application of identity management model based on OIDC authentication mechanism, a set of platforms for data interaction and unified integrated access to multiple business systems has been successfully established. It solves the problems of large time span in each system construction and the difficulty of user identity mutual trust authentication caused by inconsistent technical architecture. This method enables each system to protect user information and improve user login access ease of use.

## VI. CONCLUSION

Based on the decentralized identity authentication design idea, this paper constructs a set of identity authentication and access management service model with the core of the OIDC standard protocol, and realizes the protection of user identity information, authorization management and multi-application trusted authentication in the complex network data link. In practical application, it not only makes users more convenient to switch the system, but also reduces the security problems caused by a large amount of user information leakage, and improves the work efficiency and economic benefits of various industries and enterprises as a whole. At the same time, the model also provides a feasible solution for today's severe network security crisis situation. In the future, it will further improve and refine the current design model to achieve faster and more secure identity authentication services.

## REFERENCES

[1] Wu Shaojun. Research on decentralization of electronic competition platform based on block chain [J]. Microcomputer & Its Applications, 2019,38(12):74-78.

[2] Chen Yuxiang, Zhang Zhaolei, Zhuo Jian, Peng Di, Liu Dijun. Identity management research based on blockchain [J]. Microcomputer & Its Applications,2018,37(07):22-26.

[3] Peng Yongyong,Zhang Xiaotao. Research on Key Technologies of trusted identity authentication based on blockchain application mode [J]. Net Security Technologies and Application,2018(02):36-37.

[4] Liberty Alliance Project. Liberty Architecture Over-View[R]. California:Liberty Alliance,2003

[5] Weng Qi. A scheme of digital identity authentication based on blockchain [D]. Xidian University,2019.

[6] LIU Jianhua,WANG Xiaolei. A framework of unified identifier authentication service on public network [J]. Journal of Xi ' an Institute of Posts and Telecommunications,2014,19(02):98-101.

[7] WU De, YING Yi, MAO Dao-he. Design and Optimization of Authentication and Authorization Scheme Based on OAuth2.0 Protocol [J]. computer engineering & Software,2018,39(10):10-13.

[8] Lu Jintian. Improved openid connect protocol and its security analysis [J]. Journal of Computer Applications,2017,37(05):1347-1352.

[9] Meng Bo , Zhang Jinli, Lu Jintian. Automatic Analysis of Authentication of OpenID Connect Protocol Based on the Computational Model [J]. Journal of South-Central University for Nationalities(Natural Science Edition),2016,35(03):123-129.