

Internet Engineering Task Force	Y. Liu
Internet Draft	Z. Li
Intended status: Experimental	B. Zhang
Expires: August 10, 2022	J. Guo
China Academy of Information and Communications Technology	W. Shi
	J. Xie
	February 10, 2022

BID Protocol Specification
draft-liu-bid-protocol-specification-00

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

This Internet-Draft will expire on July 10, 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document provides an overview of the principles and

specifications of the BID (Blockchain-based Identifier) and its
relationship with BIF (National Collaborative & Innovative
Liu, et al. Expires August 10, 2022 [Page 1]

Table of Contents

1.	Introduction.....	2
1.1.	Conventions Used in This Document.....	3
2.	BID Identifier.....	3
3.	BID Documentation.....	4
4.	BID Method.....	8
4.1.	Create.....	8
4.2.	Update.....	8
4.3.	Read.....	8
4.4.	Deactivate.....	8
4.5.	Recovery.....	8
5.	Security Considerations.....	8
5.1.	Security Consideration.....	8
5.2.	Privacy Consideration.....	9
6.	IANA Considerations.....	9
7.	References.....	9
7.1.	Normative References.....	9
7.2.	Informative References.....	9
8.	Acknowledgments.....	9

[1. Introduction](#)

Decentralized identifiers (DIDs) [[W3C-DID](#)] are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are Uniform Resource Identifiers (URIs) that associate a DID subject with a DID document allowing trustable interactions associated with that subject.

BID is an exploration of new identification system research conducted by China Academy of Information and Communication Technology (CAICT) according to W3C DIDs specification. Its purpose is to build a set of independent rights controllable, data and privacy security, flexible and easy to use new identification systems. According to the W3C DIDs specification, BID is a new distributed identifier based on blockchain, which is oriented to

various entities (people, things, organizations, etc.) and digital objects, and provides Self-Sovereign Identity (SSI) services for people, devices, and virtual objects. It can be used for the owner
Liu, et al. Expires August 10, 2022 [Page 2]

to prove his control via the BID and the authentication without relying on other external organizations. BID is permanent, globally resolvable, cryptographically verifiable, and decentralized. Compared with traditional domain names and industrial Internet identifiers, it does not rely on centralized institutions, but completes the registration, resolution and distribution of identifier through blockchain.

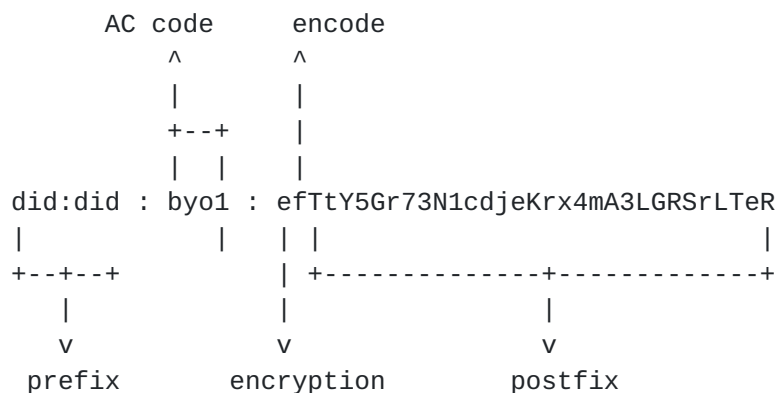
According to the W3C naming conventions, the BID namespace is "bid". DID must be prefixed with "did:bid". According to the DID specification, this string must be lowercase. The remainder of the DID is generated by a specific algorithm. Take a BID identifier: did:bid:efTtY5Gr73N1cdjeKrx4mA3LGRSrLTeR. BID is built on the BIF-core blockchain as the base module, ensuring natural credibility due to the trusted attributes designed into the data model. Each BID identifier corresponds to a DID document, which is a JSON object that stores information about the identifier.

1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [RFC2119].

2. BID Identifier

BID is structured as following:



A BID is a simple text string consisting of three parts: 1) the "did:bid" URI scheme identifier, 2) AC code, 3) the BID method-specific identifier.

The generic BID scheme is a URI scheme conformant with [RFC3986]. The ABNF definition can be found below, which uses the syntax in [RFC5234] and the corresponding definitions for ALPHA and DIGIT. All other rule names not defined in the ABNF below are defined in [RFC3986]. All BIDs MUST conform to the BID Syntax ABNF Rules.

The BID Syntax ABNF Rules.

```
<bid>          = "did:bid:" acsn ":" method-specific-id
<acsn>         = 4(alpha / digit)
                ; Autonomous Consensus System Number
```

```
< method-specific-id > = (22,42)(alpha / digit)
```

Steps taken to generate BID address is specified as following:

1. Generate public-private key pair according to the chosen encryption method.
2. Compute hash of public key.
3. Obtain length of hash and encode method corresponding to determine the length of required byte array size. Obtain the new byte array after trimming off the trailing bytes.
4. Add encode method at the front of the byte array obtained from the previous step.
5. Add encryption method at the front of the byte array obtained from the previous step.
6. If generated BID is that of the main chain, skip to the next step. Otherwise, add corresponding AC code and ":" at the front of the byte array obtained from the previous step.
7. Add "did:bid" at the front of the byte array obtained from the previous step to obtain the complete BID.

3. BID Documentation

BID documentation follows from that of DID's, and makes some extension. Specified keywords are:

- @context: A set of rules that explain JSON-LD documents for interoperability between different DID documents.

- version: documentation version

Liu, et al.

Expires August 10, 2022

[Page 4]

- id: documentation BID
- publicKey: including
 - * id, publicKey's id
 - * type, encryption method
 - * controller, ownership of publicKey
 - * publicKeyHex, publicKey's hex encode
- authentication: BID of a publicKey, revealing the holder of the BID, who retains the control of this BID document.
- alsoKnownAs: a set of ID related to BID, including
 - * type, related identifiers' types
 - * id, related identifiers.
- extension: optional fields, including
 - * recovery, id of publicKey used to recover control when authentication privateKey is compromised or lost
 - * ttl, Time-To-Live, when resolution service requires usage of buffer
 - * delegateSign, third party signature to publicKey, used for trusted resolution, including
 - signer, id of publicKey
 - signatureValue, signature generated with publicKey's corresponding privateKey
 - * type, property type of BID documentation
 - * attributes, a set of properties, varying according to documentation's own properties
 - when type is of credential, property is verifiable credential
 - signature is generated based on credential's byte array
 - * acsns, optional field, side-chain AC code. BID documentation is the sole type not belonging to credential type. On extra, only BID documentation on main-chain can have this field, encapsulating all of the AC codes.
- service: optional field comprising service addresses, including

- * id, service address' id
- * type, string representing service type
- * serviceEndPoint, URI address
- created, mandatory field, time of creation
- updated, mandatory field, time of last update
- proof, optional field, documentation owner's signature on documentation's content, including
 - * creator, creator of proof, id of publicKey
 - * signatureValue, signature on the entire documentation except proof field

BID documentation example:

```
{
  "@context": ["https://www.w3.org/ns/did/v1"],
  "version": "1.0.0",
  "id": "did:bid:efnVUgqQFfYeu97ABf6sGm3WFtVXHZB2",
  "publicKey": [{
    "id": "did:bid:efnVUgqQFfYeu97ABf6sGm3WFtVXHZB2#key-1",
    "type": "Ed25519",
    "controller": "did:bid:efnVUgqQFfYeu97ABf6sGm3WFtVXHZB2",
    "publicKeyHex":
    "b9906e1b50e81501369cc777979f8bcf27bd1917d794fa6d5e320b1ccc4f48bb"
  }, {
    "id": "did:bid:efnVUgqQFfYeu97ABf6sGm3WFtVXHZB2#key-2",
    "type": "Ed25519",
    "controller": "did:bid:efnVUgqQFfYeu97ABf6sGm3WFtVXHZB2",
    "publicKeyHex":
    "31c7fc771eba5b511b7231e9b291835dd4ebde51cc0e757a84464e7582aba652"
  }],
}
```



```
"authentication": ["did:bid:efnVUgqQFfYeu97ABf6sGm3WFtVXHfB2#key-1"],

"extension": {

  "recovery": ["did:bid:efnVUgqQFfYeu97ABf6sGm3WFtVXHfB2#key-2"],

  "ttl": 86400,

  "delegateSign ": {

    "signer": "did:bid:efJgt44mNDewKK1VEN454R17cjs03mSG#key-1",

    "signatureValue":
"eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19"

  },

  "type": 206

},

"service": [{

  "id": "did:bid:ef24NBA7au48UTZrUNRHj2p3bnRzF3YCH#subResolve",

  "type": "DIDSubResolve",

  "version": "1.0.0",

  "serverType": 1,

  "protocol": 3,

  "serviceEndpoint": "192.168.1.23",

  "port": 8080

}],

"created": "2021-05-10T06:23:38Z",

"updated": "2021-05-10T06:23:38Z",

"proof": {

  "creator": "did:bid:efJgt44mNDewKK1VEN454R17cjs03mSG#key-1",

  "signatureValue":
"9E07CD62FE6CE0A843497EBD045C0AE9FD6E1845414D0ED251622C66D9CC927CC21
DB9C09DFF628DC042FCBB7D8B2B4901E7DA9774C20065202B76D4B1C15900"
```



```
}
```

```
}
```

4. BID Method

4.1. Create

By creating a socket, a BID documentation creation is achieved, while supporting http POST method. When creating BID documentation, signer inside proof field must be same as authentication field's public key for creation to be considered successful.

4.2. Update

By updating a socket, a BID documentation update is achieved, while supporting http POST method. update is not authenticated to update authenticate field. When updating BID documentation, signer inside proof field must be same as authentication field's public key for update to be considered successful.

4.3. Read

Inquire BID documentation according to BID, while supporting http POST method. Return value is JSON string from BID documentation.

4.4. Deactivate

Deactivate revokes BID documentation, while supporting http POST method. Revoked BID documentation is empty, not deleted. deactivated BID documentation's proof field's signer has to be recovery field's public key.

4.5. Recovery

Recovery modifies authentication and public key fields in BID documentation, while supporting http POST. Proof field's signer must be recovery field's public key for recovery to be effective.

5. Security Considerations

5.1. Security Consideration

DDOS: BID is based on blockchain, which is difficult for DDOS attack at the first place.

Privacy data: in a BID framework, all user-related privacy data is stored locally. Only encrypted hash or string is on the chain, so it can be assumed that de-decryption is not possible.

Consensus: two layers of consensus consisting of DPOS and PBFT are

used to ensure each replica's stability.

Liu, et al.

Expires August 10, 2022

[Page 8]

5.2. Privacy Consideration

All privacy data is stored locally, went through sorting, compression, encoding to ensure privacy. Under preceding measures, privacy data is guranteed not to be compromised.

6. IANA Considerations

7. References

7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [W3C-DID] W3C, W3C., "Decentralized Identifiers (DIDs) v1.0", February 2020, <<https://www.w3.org/TR/did-core/>>.

7.2. Informative References

- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, [RFC 3986](#), DOI 10.17487/RFC3986, January 2005, <<https://www.rfc-editor.org/info/rfc3986>>.
- [RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), DOI 10.17487/RFC5234, January 2008, <<https://www.rfc-editor.org/info/rfc5234>>.

8. Acknowledgments

This document is based on an identifier application of DIDs, the author would like to thank J. Xie who suggested improvements and provided many invaluable comments. This document are individual submissions, based on the work done in [RFC 7553](#).

This document was prepared using 2-Word-v2.0.template.dot.

Yuanchao Liu
CAICT
No.52 Huayuan North Road, Haidian District

Phone: +86 188 0011 6727
Email: liuyuanchao@caict.ac.cn

Zhiping Li
CAICT
No.52 Huayuan North Road, Haidian District

Phone: +86 185 1107 1386
Email: lizhiping@caict.ac.cn

Bo Zhang
CAICT
No.52 Huayuan North Road, Haidian District

Phone: +86 153 8346 0204
Email: zhangbo3@caict.ac.cn

Jian Guo
CAICT
No.52 Huayuan North Road, Haidian District

Phone: +86 189 4004 7983
Email: guojian@caict.ac.cn

Weijun Shi
CAICT
No.52 Huayuan North Road, Haidian District

Phone: +86 131 1607 3615
Email: 1525109982@qq.com

Jiagui Xie
CAICT
No.52 Huayuan North Road, Haidian District

Phone: +86 150 0138 5070
Email: xiejiagui@caict.ac.cn

