BSN-DDC Network
DID-SDK Instructions

V1.0

Red Date Technology

December 2021

1 Document Description

This document explains the function of the DID-SDK. Platform Owners can read this document for connecting to the BSN-DDC Network. As the on-chain identity of Platform Owners, the BSN DID is associated with a Platform Owner's service activation certificate, chain accounts, and the chain accounts of their end users. It is also the basic identity for Platform Owners to deploy DDC applications and manage business. The SDK contains three functions: DID registration, DID verification, and key update. Platform Owners only need to register DID once and they should properly store and backup the private key that controls the BSN DID. In case the private key is lost or stolen, a new private key for the BSN DID can be regenerated by the key update function.

2 Parameter Format Standard

❑ Time

The time parameter is a string in the form of yyyy-MM-dd HH:mm:ss, for example, 2021-05-25 12:30:59 means 12:30:59 on May 25, 2021.

❑ Exception return

When the SDK is processing the function and an error occurs, a runtime exception containing the specific error message will be

returned.

3 Function Description

Platform Owners shall complete the DID registration before signing the BSN-DDC Platform Agreement and then keep the generated private key and DID information.

3.1 DID Registration

During the DID registration, public and private keys and DID information will be generated offline. Then the SDK will call the API and store the corresponding DID document on the chain.

- Method definition: DidDataWrapper createDid();
- Request parameters: none
- Response parameters:

Field name	Field	Type	Mandatory
DID	did	String	Yes
DID signature value	didSign	String	Yes
Authentication public and private keys	authKeyInfo	KeyPair	Yes
Recovery public and private keys	recyKeyInfo	KeyPair	Yes
DID document	document	DocumentInfo	No
KeyPair			
Private key information	privateKey	String	Yes

Public key information	publicKey	String	Yes
Encryption algorithm	type	String	Yes
DocumentInfo			
DID	did	String	Yes
Version	version	String	Yes
Created time	created	String	Yes
Updated time	updated	String	No
Authentication public key	authentication	PublicKey	Yes
Authentication public key	recovery	PublicKey	Yes
Signature information	proof	Proof	Yes
PublicKey			
Public key information	publicKey	String	Yes
Encryption algorithm	type	String	Yes
Proof			
Signature value	signValue	String	Yes
Signature algorithm	type	String	Yes
DID of the signer	creator	String	Yes

3.2 DID Verification

Platform Owners need to submit the DID and DID signature value when activating the DDC service and creating chain accounts. Following this step, BSNDA will verify the DID. In order to make the activation process easier, Platform Owners can verify the DID information in advance.

- Method definition: Boolean verifyDIdSign(DidSign didSign);
- Request parameters:

Field name	Field	Type	Mandatory
DID	did	String	Yes
DID signature value	didSign	String	Yes

- Response parameters:

Field name	Field	Type	Mandatory
		Boolean	Yes

3.3 Key Update

If Platform Owners lose or expose the authentication private key they may generate a new pair of authentication public and private keys by “Key Update" method. The DID will not be changed after the key is updated which will not affect the DDC service.

- Method definition: KeyPair resetDidAuth(ResetDidAuth restDidAuth);
- Request parameters:

Field name	Field	Type	Mandatory
DID	did	String	Yes
Authentication public and private keys	primaryKey	KeyPair	No
Recovery public and private keys	recoveryKey	KeyPair	Yes
KeyPair			
Private key	privateKey	String	Yes

Public key	publicKey	String	Yes
Encryption algorithm	type	String	Yes

- Response parameters:

Field name	Field	Type	Mandatory
New authentication public and private keys	keyInfo	KeyPair	Yes
KeyPair			
Private key	privateKey	String	Yes
Public key	publicKey	String	Yes
Encryption algorithm	type	String	Yes