BSN-DDC 基础网络

DID-SDK 说明手册

V1.0

北京红枣科技有限公司

2021 年 12 月

1 文档说明

本文档对 DID-SDK 的方法进行说明，平台方在对接 BSN-DDC 基础网络过程中可阅读参考。BSN DID 是平台方的链上身份凭证标识，关联平台方的业务开通凭证、链账户以及其下终端用户的链账户，是平台方开展 DDC 应用和管理业务的基础标识。SDK 内包含注册 DID、更新密钥、验证 DID 三个方法，平台方只需注册一次 DID 即可，所以需妥善保存和备份好 BSN DID 的控制私钥，如私钥丢失或泄漏，通过更新密钥方法重新生成 BSN DID 的控制私钥。

2 参数格式标准

❑ 时间

格式为 yyyy-MM-dd HH:mm:ss 形式的字符串，例如: 2021-05-25 12:30:59 表示 2021 年 5 月 25 日 12 时 30 分 59 秒。

❑ 返回异常

当 SDK 处理功能逻辑出错时，会抛出相应的运行时异常，包含具体的错误信息。

3 方法说明

平台方在线下签署协议之前应完成 DID 的注册，注册 DID 后生成的私钥和 DID 标识符请保存牢记。

3.1 注册 DID

注册 DID 过程中会离线生成公私钥和 DID 信息，然后生成 DID 对应的 Document 并通过远程调用 API 将 DID Document 上链存储。

- 方法定义：DidDataWrapper createDid();
- 输入参数：无
- 输出参数：

字段名	字段	类型	必传
DID	did	String	是
DID 签名值	didSign	String	是
主公私钥	authKeyInfo	KeyPair	是
备公私钥	recyKeyInfo	KeyPair	是
DID 文档	document	DocumentInfo	否
KeyPair			
私钥信息	privateKey	String	是
公钥信息	publicKey	String	是
加密算法	type	String	是
DocumentInfo			
DID	did	String	是
版本号	version	String	是
创建时间	created	String	是
更新时间	updated	String	否
主公钥	authentication	PublicKey	是
备公钥	recovery	PublicKey	是

签名信息	proof	Proof	是
PublicKey			
公钥信息	publicKey	String	是
加密算法	type	String	是
Proof			
签名值	signValue	String	是
签名算法	type	String	是
签名者的 DID	creator	String	是

3.2 验证 DID

平台方在开通 DDC 业务、创建链账户过程中，都需要上送自己的 DID 和 DID 签名值，由 BSN 联盟对数字身份进行验证。为保证业务流程的顺畅，平台方可提前对自己的 DID 进行验证。

- 方法定义：Boolean verifyDIdSign(DidSign didSign);
- 输入参数：

字段名	字段	类型	必传
DID	did	String	是
DID 签名值	didSign	String	是

- 输出参数：

字段名	字段	类型	必传
		Boolean	是

3.3 更新密钥

平台方的主私钥丢失或者泄漏，通过“更新密钥”重新生成一对

主公私钥。密钥更新后，DID 标识符不会改变所以不会影响 DDC 业务。

- 方法定义：KeyPair resetDidAuth(ResetDidAuth restDidAuth);
- 输入参数：

字段名	字段	类型	必传
DID	did	String	是
主公私钥	primaryKey	KeyPair	否
备公私钥	recoveryKey	KeyPair	是
KeyPair			
私钥	privateKey	String	是
公钥	publicKey	String	是
加密算法	type	String	是

- 输出参数：

字段名	字段	类型	必传
新公私钥	keyInfo	KeyPair	是
KeyPair			
私钥	privateKey	String	是
公钥	publicKey	String	是
加密算法	type	String	是