# Textile现有账户管理



## 全局唯一助记符“ [mnemonic phrase](https://en.bitcoin.it/wiki/Seed_phrase)”原理

分布式钱包根据密钥之间是否有关联可把钱包分为两类：nondeterministic wallet 和 deterministic wallet；

nondeterministic wallet：密钥对之间没有关联；

deterministic wallet: 密钥对由一个原始的种子主密钥推导而来。最常见的推导方式是树状层级推导 (hierarchical deterministic) 简称 HD

目前Textile Wallet采用的是钱包类型为：deterministic wallet。

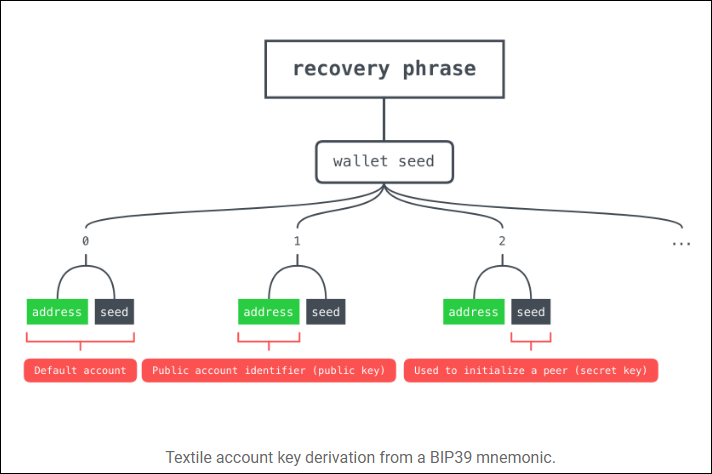
### deterministic wallet BIP32标准

密钥对由一个原始的种子主密钥推导而来。最常见的推导方式是树状层级推导 (hierarchical deterministic) 简称 HD。deterministic wallet 基于 BIP32 (Bitcoin Improvement Proposal 32) 标准实现，通过一个共同的种子维护 n 多私钥，种子推导私钥采用不可逆哈希算法，在需要备份钱包私钥时，只备份这个种子即可（大多数情况下的种子是通过 BIP44 生成了助记词，方便抄写），在支持 BIP32, BIP44 标准的钱包只需导入助记词即可导入全部的私钥；

### deterministic wallet BIP39标准

BIP39 标准就是为了解决助记词的需求，通过随机生成 12 ~ 24 个容易记住的单词，单词序列通过 PBKDF2 与 HMAC-SHA512 函数创建出随机种子作为 BIP32 的种子；BIP39 标准定义了钱包助记词和种子生成规则，通过九个步骤即可生成钱包助记词和种子：步骤 1~6 生成助记词、步骤 7~9 把前六步生成的助记词转化为 BIP32 种子；

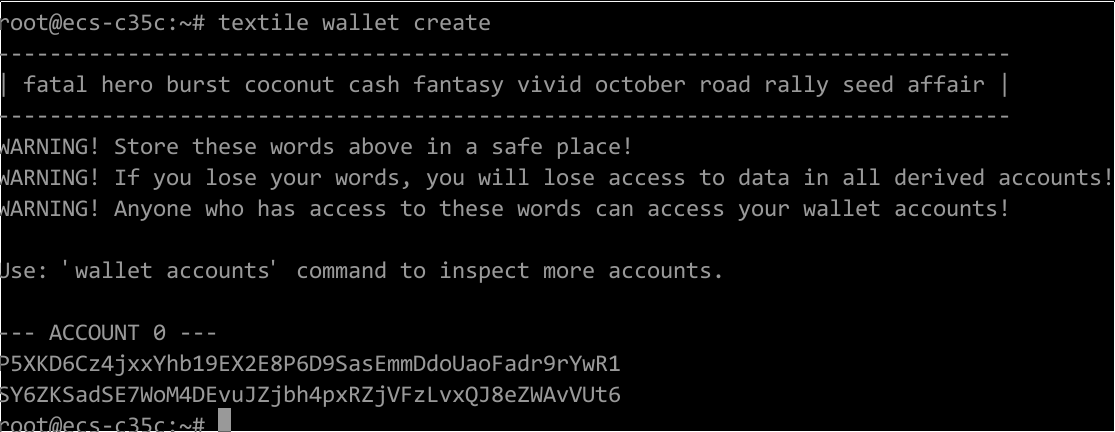
## 钱包Textile Wallet实现



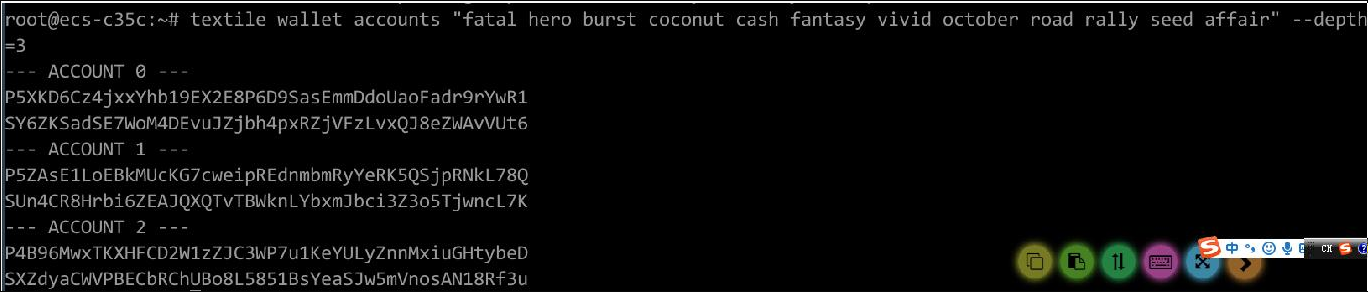
使用全局唯一的助记符为用户生成公私钥：公钥作为address、私钥作为seed。

由Textile Wallet默认生成的全局唯一的助记符来生成一组或者多组树形层次化的公私钥。

目前实现为：默认创建一个账号公私钥对，默认创建唯一的助记符和“Account 0”公私钥：



通过助记符创建分层的3对公私钥：

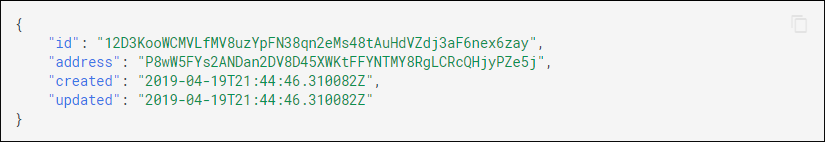


助记符和后面的公私钥是一对一的生成关系，通过助记符可以唯一的生成“Account 0”的公私钥，“Account 0可以计算得出Account 1的公私钥”，“Account 1可以计算得出Account 2的公私钥”，构成父亲-儿子-孙子的树形关系。

## Account节点

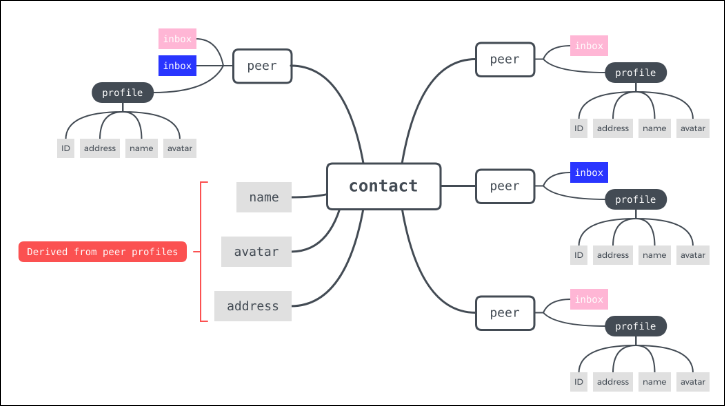
### Textile账户节点，在PC、Phone等端侧服务于Textile APP

### 向Cafe节点、其他的Account节点发布由[公钥-即账户地址、IPFS节点ID]组成的用户节点通讯信息，Peer profile:



## Cafe节点

用户所在的Account节点将通讯录信息发送到Cafe节点，由Cafe节点负责在网络内快速扩散，加速相同用户不同设备节点、不同用户建立组群的账户路由性能。



# 华为现有账户管理

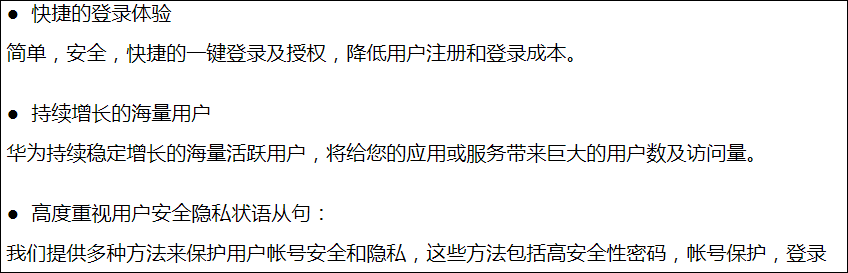
## 开发者联盟开发指导Web

<https://developer.huawei.com/consumer/cn/service/hms/catalog/huaweiid_dp.html?page=hmssdk_huaweiid_introduction_dp>

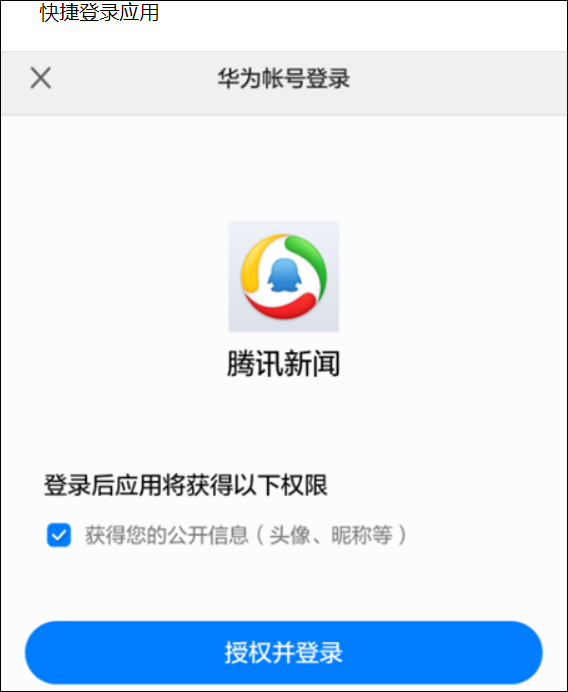
<https://developer.huawei.com/consumer/cn/devservice/doc/31107>

## 华为账号使用

### 华为帐号适用于访问所有华为服务。华为帐号为开发者提供了简单，安全的登录授权功能，方便用户快捷登录



### 服务场景



## 开发者环境配置步骤

### 注册认证成为开发者

### 配置应用签名

### 创建产品和应用

### 开通账号服务

### 下载SDK

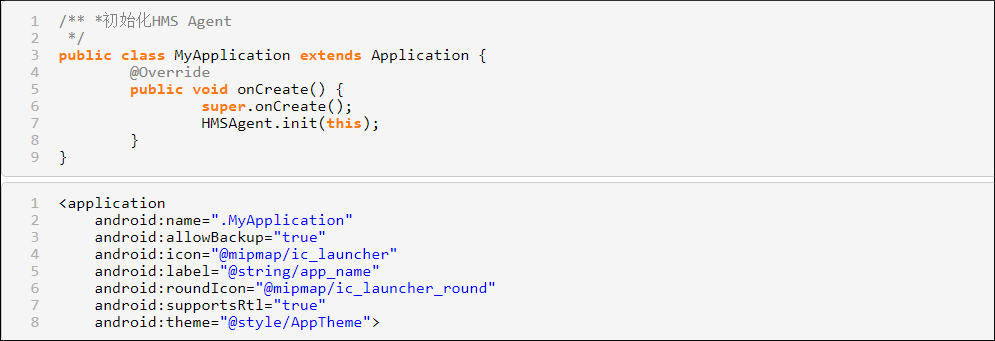
### 集成Android Studio开发工具

## 华为账号向APP提供的API

### 初始化代理

HMS Agent 套件提供了对HMS SDK原生接口的二次封装，处理了部分必要的接入逻辑而不再将它们暴露给开发者，使用封装后的Agent接口接入HMS SDK，可大大提升接入效率，降低出错几率。

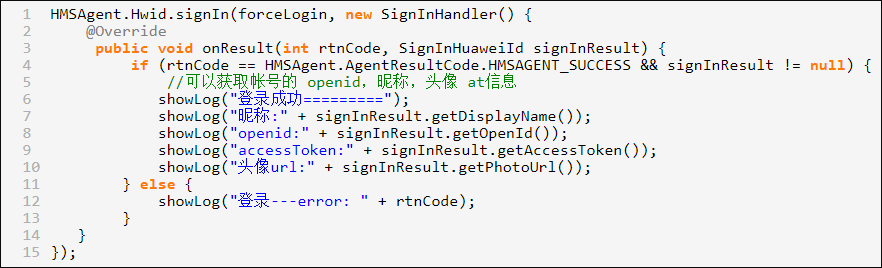
示例代码如下：



### 调用signIn接口函数

**接口名：**void HMSAgent.Hwid.signIn(forceLogin, new SignInHandler())，简称signIn接口，接口详细定义请参见**signIn。**

**示例代码：**

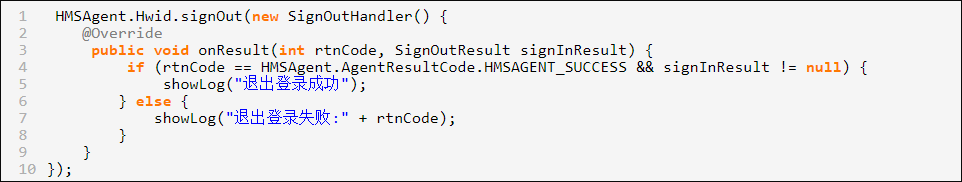


调用此API返回用户全局唯一的OpenID、昵称、头像图片。

### 调用signOut接口函数

**接口名：**void HMSAgent.Hwid.signOut(new SignOutHandler()，简称signOut接口，接口详细定义请参见**signOut。**

**示例代码：**



# Textile使用华为账号的方案



## Textile APP-Photos开发环境集成华为账号管理SDK

目前华为账号管理服务已经支持，在Android studio中直接安装华为提供的HWS插件即可。

## 使用华为账号管理API获取唯一的用户OpenID

Textile Photos源码调用HWS signIn接口函数，获取用户的OpenID。如果华为手机使用的用户未登陆华为账号，需要提示用户通过手机的原生华为账号管理程序登陆华为账号。

## 将OpenID转化为Textile需要的全局唯一助记符

Textile Photos源码将获取的用户OpenID作为触发因子，通过特定算法转化为Textile需要的全局唯一助记符，直接用于Textile wallet的计算用户公私钥使用。

### deterministic wallet BIP32标准

密钥对由一个原始的种子主密钥推导而来。最常见的推导方式是树状层级推导 (hierarchical deterministic) 简称 HD。deterministic wallet 基于 BIP32 (Bitcoin Improvement Proposal 32) 标准实现，通过一个共同的种子维护 n 多私钥，种子推导私钥采用不可逆哈希算法，在需要备份钱包私钥时，只备份这个种子即可（大多数情况下的种子是通过 BIP44 生成了助记词，方便抄写），在支持 BIP32, BIP44 标准的钱包只需导入助记词即可导入全部的私钥；

### deterministic wallet BIP39标准

BIP39 标准就是为了解决助记词的需求，通过随机生成 12 ~ 24 个容易记住的单词，单词序列通过 PBKDF2 与 HMAC-SHA512 函数创建出随机种子作为 BIP32 的种子；BIP39 标准定义了钱包助记词和种子生成规则，通过九个步骤即可生成钱包助记词和种子：步骤 1~6 生成助记词、步骤 7~9 把前六步生成的助记词转化为 BIP32 种子；

### Textile Wallet修改方案

目前Textile Wallet的密钥管理算法采用“基于Stellar的SLIP-0010实现的BIP32分层确定性钱包”，开源地址：<https://github.com/satoshilabs/slips。可以将华为ID服务返回的OpenID直接或者计算hash值作为BIP32>种子，然后通过BIP44生成助记符作为Textile Wallet的助记符“[mnemonic phrase](https://en.bitcoin.it/wiki/Seed_phrase)”，后面Textile Wallet层次化的公私钥生成策略保持不变。

## 将HWS SDK-API返回的用户昵称、头像直接用于Account节点账户管理，删除Textile Photos原有的昵称、头像收集界面

## Textile Account节点其它的流程和Cafe节点全部的流程保持不变，对于使用华为账号无感知