JDChain整合ssh-keygen

# 简介

SSH 为 Secure Shell的缩写，由 IETF 的网络小组（Network Working Group）所制定；它是建立在应用层基础上的安全协议。

SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

ssh-keygen工具可以利用ssh协议快速的生成公私钥对文件。JDChain系统进行了技术融合，可以让用户方便的使用ssh-keygen工具生成的公私钥对，实现与原有公私钥的无缝集成。

关键源码：

相关操作视频地址：<https://3.cn/aQoICkT>

# 操作步骤

本文假设几个前提：

1. 基于：CentOS Linux release 7.3构建。
2. 假定JDChain区块链环境已经构建完成，并假定区块链浏览器地址为：<http://192.168.151.39:18081>
3. 基于<https://github.com/blockchain-jd-com/jdchain-starter> 的master主干来辅助完成样例；

## 安装ssh-keygen

命令如下：

yum install -y ssh-keygen

## jdchain-starter连接网关配置

修改SDKDemo\_Constant.java中网关IP和端口，以及绑定的peer节点的公私钥信息。

## 密钥类型-RSA

### 生成基于RSA的公私钥

ssh-keygen创建公钥-私钥对

在指定目录下生成rsa密钥, 并指定注释为“zgw”, 实现示例:

[root@localhost ~]# ssh-keygen -t rsa -f /export/ssh/rsa -C zgw

在/export/ssh路径下生成公私钥文件：rsa和rsa.pub。

### 基于此公私钥在JDChain账本上注册用户

打开SshKeyTest.java中的registerUser\_Rsa\_ByExistPubAndPrivKey()样例，并将其中的公私钥替换为新生成的公私钥信息，然后执行，观察区块链浏览器的结果变化。

## 密钥类型-ECDSA

### 生成基于ECDSA的公私钥

ssh-keygen创建公钥-私钥对

在指定目录下生成rsa密钥, 并指定注释为“zgw”, 实现示例:

[root@localhost ~]# ssh-keygen -t ecdsa -f /export/ssh/ecdsa -C zgw

在/export/ssh路径下生成公私钥文件：ecdsa和ecdsa.pub。

### 基于此公私钥在JDChain账本上注册用户

打开SshKeyTest.java中的registerUser\_ecdsa\_ByExistPubAndPrivKey()样例，并将其中的公私钥替换为新生成的公私钥信息，然后执行，观察区块链浏览器的结果变化。

## 密钥类型- ed25519

### 生成基于ed25519的公私钥

ssh-keygen创建公钥-私钥对

在指定目录下生成rsa密钥, 并指定注释为“zgw”, 实现示例:

[root@localhost ~]# ssh-keygen -t ed25519 -f /export/ssh/ed25519 -C zgw

在/export/ssh路径下生成公私钥文件：ed25519和ed25519.pub。

### 基于此公私钥在JDChain账本上注册用户

打开SshKeyTest.java中的registerUser\_ ed25519\_ByExistPubAndPrivKey()样例，并将其中的公私钥替换为新生成的公私钥信息，然后执行，观察区块链浏览器的结果变化。