简介

- zero-knowledge proof(零知识证明),零知识证明可提供匿名性和无关联性
- Idemix是一个加密协议套件，它提供强大的身份验证以及隐私保护功能，如匿名，无需披露交易者身份即可进行交易，以及不可链接性，即单个身份发送多个交易的能力，而不会泄露 交易是通过相同的身份发送的
- 该工具可用于为基于MSP的身份混合器创建配置文件。 有两个命令可用，一个用于创建新的CA密钥对，另一个用于使用以前生成的CA密钥创建MSP配置。

编译安装

```
$ cd $GOPATH/src/github.com/hyperledger/fabric
$ make idemixgen
$ cp build/bin/idemixgen /usr/bin
```

参数说明

```
Utility for generating key material to be used with the Identity
Mixer MSP in Hyperledger Fabric

Flags:
  -h, --help                    Show context-sensitive help (also
try --help-long and --help-man).
      --output="idemix-config"  The output directory in which to
place artifacts

Commands:
  help [<command>...]
    Show help.

  ca-keygen
    Generate CA key material

  signerconfig [<flags>]
    Generate a default signer for this Idemix MSP

  version
    Show version information
```

```
usage: idemixgen signerconfig [<flags>]

Generate a default signer for this Idemix MSP

Flags:
   -h, --help               Show context-sensitive help (also try --
help-long and --help-man).
   -u, --org-unit=ORG-UNIT  The Organizational Unit of the default
signer
   -a, --admin              Make the default signer admin
   -e, --enrollment-id=ENROLLMENT-ID
                            The enrollment id of the default signer
   -r, --revocation-handle=REVOCATION-HANDLE
                            The handle used to revoke this signer
```

密钥生成

```
$idemixgen ca-keygen

#生成的文件如下
- /ca/
    IssuerSecretKey
    IssuerPublicKey
    RevocationKey
- /msp/
    IssuerPublicKey
    RevocationPublicKey
- /user/
    SignerConfig
```