ICS 35.040

L 80

# 团 体 标 准

T/SCCIA 006—2020

# 聚龙链密码材料生成工具接口标准及安全要求

JulongChain cryptography material generation interface specification and security requirements

2020－01－07 发布　　2020－01－08 实施

深圳市商用密码行业协会　发布

# 目　　次

# 前　言

本标准依据GBT 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由深圳市商用密码行业协议提出并归口。

本标准起草单位：深圳市文鼎创数据科技有限公司、鼎铉商用密码测评技术（深圳）有限公司、深圳市电子商务安全证书管理有限公司。

本标准起草人：李振明、刘锡锋、刘伟丰、冯灼坤、苏年乐、周辉、罗六飞。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

# 聚龙链密码材料生成工具接口标准及安全要求

## 1 引言

聚龙链平台是一个开源联盟链区块链底层技术平台。该项目旨在使用符合国家密码管理要求的国密算法和证书体系，打造一个数据防篡改、账本分布共享、系统安全可靠的开源区块链基础设施平台，为金融、政务、能源等重点领域区块链应用提供平台支撑。

## 2 范围

本标准规定了聚龙链中测试证书及私钥的生成接口，规定了生成接口应当遵循的安全要求。

本标准适用于提供区块链启动必须的密码材料，以便快速部署运行聚龙链。

## 3 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

[1] 安全芯片密码检测准则:GM/T 0008-2012[S].国家密码管理局,2012.

[2] 密码模块安全技术要求:GM/T 0028-2014[S].国家密码管理局,2014.

[3] 密码模块安全检测要求:GM/T 0039-2015[S].国家密码管理局,2015.

[4] SM2 椭圆曲线公钥密码算法:GM/T 0003-2012[S].国家密码管理局,2012.

[5] 随机性检测规范:GM/T0005-2012[S].国家密码管理局,2012.

## 4 术语与定义

下列术语和定义适用于本文件。

### 4.1 密码材料

即证书与私钥，证书有两种类型，一种是节点之间通讯的TLS/SSL证书，另一种是各组织和成进行身份验证和权限控制的 MSP 证书。

### 4.2 cryptogen

即聚龙链密码材料生成工具，是一个命令行工具，可以带参数运行。工具所生成的所有密码材料，如无额外指明，默认为 PEM 编码。

### 4.3 配置文件

作为输入参数给聚龙链密码材料生成工具使用，用于按要求生成密码材料。

### 4.4 PEM 编码

PEM是OpenSSL和许多其他SSL工具的标准格式，全称是Privacy Enhanced Mail。

### 4.5 MSP

Membership Service Provider。成员服务提供者：抽象的实现成员服务（身份验证，证书管理等）的组件，实现对不同资源进行基于身份验证的权限验证。

### 4.6 CSP

即加密服务提供者(Cryptographic Service Provider)。

### 4.7 节点

区块链网络的逻辑通信主体。

### 4.8 Consenter 节点

架构中的共识服务角色，负责接收包含背书签名的交易，对未打包的交易进行排序生成区块，广播给node节点。

### 4.9 Node 节点

分为记账节点和背书节点两种角色，负责验证从 consenter 节点区块里的交易，维护状态数据和账本的副本。充当背书节点时，执行交易并对结果进行签名背书

### 4.10 组织

代表一组拥有共同信任的根证书（可以为根CA证书或者中间CA证书）的成员。

## 5 密码材料生成工具接口规范

聚龙链密码材料生成工具，是一个命令行工具，可根据配置文件快速生成密码材料。
本章节内容主要介绍密码材料生成工具支持的命令行接口以及参数内容。

### 5.1 命令接口规范

#### 5.1.1 help

返回工具简介和支持的命令，例：

```
Utility for generating BCIA key material
Flags:
  --help  Show context-sensitive help. e.g. generate --help
Commands:
  help
    Show help
  genkey[opts]
    Generate key material
  gencsr[opts]
    Generate certificate signing request
  extendkey[opts]
    Extend existing network
```

```
showtemplate
  Show the default configuration template
version
  Show version information
```

#### 5.1.2 --help

上下文敏感的帮助命令。如命令参数只包含一个–help，则与 help 命令行为一致。若是其他支持查询帮助的命令，如 genkey 和 extendkey，则返回 genkey 和 extendkey 对应的帮助信息。如不支持查询帮助，没有额外参数可配置的简单命令，如 help，version 和 showtemplate，则忽略 --help。

#### 5.1.3 version

返回编译 cryptogen 版本，当前开发语言版本，当前操作系统版本，例：

```
cryptogen:
Version: development build
Java version: 1.8.0_171
OS/Arch: Mac OS X/x86_64
```

#### 5.1.4 showtemplate

返回工具不指定配置文件时，默认的密码材料生成配置。

#### 5.1.5 genkey

根据配置文件生成密码材料

- --config：指定生成配置文件。
- --output：指定生成目录，默认为当前命令行执行目录。
- --help：打印帮助信息。

#### 5.1.6 gencsr

根据配置文件生成 CSR 证书签名请求文件，用于发送给 CA 机构颁发证书。

- --config：指定生成配置文件。
- --output：指定生成目录，默认为当前命令行执行目录。
- --help：打印帮助信息。

#### 5.1.7 extendkey

在原来密码材料的基础上生成新配置的密码材料。指定已生成的密码材料目录和新修改的配置文件，工具仅生成新的节点的密码材料，其他密码材料不做修改。

- --config：同 genkey
- --input：genkey生成的旧密码材料目录，并以此为输出目录
- --help：打印帮助信息

#### 5.1.8 其他输入

返回 help 命令结果。

## 6 密码材料配置文件规范

密码材料生成工具负责生成网络中所有身份所需的密码材料，所依赖的配置文件确定需要生成多少证书，所需证书的特性以及相关私钥。

配置文件指定 consenterOrgs、nodeOrgs、consenterOrgs.ca、nodeOrgs.ca 4 个组织，其中 consenterOrgs、nodeOrgs 用于测试阶段，其中 consenterOrgs.ca、nodeOrgs.ca 用于正式环境。

本章节主要描述密码材料生成工具配置文件字段的内容和约束。

### 6.1 consenterOrgs 配置

使用 consenterOrgs 表示配置 consenter 集群，为数组结构（yaml 用“-”作为前缀表示每个数组成员）。

consenterOrgs 的每个成员都代表一个组织下的 consenter 集群,每个组织都可以通过 specs 配置多个 consenter。

#### 6.1.1 name 配置

必选配置。

指定该组织的名字。仅作为标识使用，不会出现在密码材料生成物上。

#### 6.1.2 domain 配置

必选配置。

指定该组织的域名。将作为该节点的生成物的文件夹名，和该节点下所有相关证书（包括 ca 和 consenter）的根域名。

#### 6.1.3 specs 配置

可选配置。

用于指定一个或多个 consenter 证书相关配置，为数组结构。指定多个 specs，将生成多个 consenter 节点证书。

##### 6.1.3.1 hostname 配置

可选配置。

用于指定 consenter 证书次级域名,用于生成证书 DN（若 commonName 未指定）。若不指定则使用默认值“consenter{num}”，其中{num}按照声明顺序递增，从 0 开始。

##### 6.1.3.2 commonName 配置

可选配置。

用于指定 consenter 证书的 DN 名，若未指定，则使用默认名字{HostName}.{Domain}。启动 HostName为 6.1.3.1 的 hostname，domain 为 6.1.2 的 domain。

##### 6.1.3.3 sans 配置

可选配置。

指定 consenter X509证书的一个或多个 Subject 可选名，数组结构。可选名可以使用模版变量 {{.Hostname}}, {{.Domain}}, {{.CommonName}}。若使用的是IP地址，也可以被识别；其他变量将会被识别为DNS名。例：

```
sans:
  - "bar.{{.Domain}}"
```

- "altfoo.{{.Domain}}"
- "{{.Hostname}}.org6.net"
- 172.16.10.31

#### 6.1.4 ca 配置

可选配置。

为该 consenter 节点的 CA 证书配置 Subject 和 DN。

ca 配置继承 specs 的单项配置，所以同样支持 hostname，commonName 和 sans 配置，除了 hostname 默认名变为 ca 之外。

##### 6.1.4.1 hostname 配置

除了默认值为“ca”外，同 6.1.3.1 Specs 的 hostname 配置。

##### 6.1.4.2 commonName 配置

同 6.1.3.2 Specs 的 commonName 配置。

##### 6.1.4.3 sans 配置

同 6.1.3.3 Specs 的 sans 配置。

##### 6.1.4.4 country 配置

可选配置。

用于节点 CA 证书 Subject 的 C 字段。

##### 6.1.4.5 province 配置

可选配置。

用于节点 CA 证书 Subject 的 ST 字段。

##### 6.1.4.6 locality 配置

可选配置。

用于节点 CA 证书 Subject 的 L 字段。

##### 6.1.4.7 organizationalUnit 配置

可选配置。

用于节点 CA 证书 Subject 的 OU 字段。

##### 6.1.4.8 streetAddress 配置

可选配置。

用于节点 CA 证书 Subject 的 STREET 字段。

##### 6.1.4.9 postalCode 配置

可选配置。

用于节点 CA 证书 Subject 的 POSTAL_CODE 字段。

#### 6.1.5 template 配置

可选配置。
此配置将快速的生成多个节点，默认节点名的格式为 consenter{num}，num从 0 开始逐渐递增。

##### 6.1.5.1 count 配置

必选配置。
指定模版节点数量。

##### 6.1.5.2 start 配置

可选配置。
节点名序号将从 start 号开始，默认为0。

##### 6.1.5.3 hostname 配置

可选配置。
指定模版节点的名字，默认为 consenter。

##### 6.1.5.4 sans 配置

可选配置。
见 6.1.3.3 sans 配置。

### 6.2 nodeOrgs 配置

#### 6.2.1 name 配置

同 consenterOrgs 6.1.1。

#### 6.2.2 domain 配置

同 consenterOrgs 6.1.2。

#### 6.2.3 specs 配置

同 consenterOrgs 6.1.3。

#### 6.2.4 ca 配置

同 consenterOrgs 6.1.4。

#### 6.2.5 template 配置

除了默认名从 consenter 变为 node 之外，同 consenterOrgs 6.1.5。

#### 6.2.6 enableNeedOUs 配置

可选配置。
默认为 false。

1. 如果为 true，该 node 节点的 MSP 证书 Subject 的 OU 字段将增加“node”（如果是服务器证书），或者增加“client”（如果是用户证书）
2. 如果为 true，将导出该节点的 MSP 的 config.yaml 文件。

### 6.2.7 users 配置

可选配置。

增加除 Admin 用户之外，User 用户的个数。默认为 0，即只有 Admin 用户。

### 6.3 consenterOrgs.ca 配置

同 consenterOrgs

### 6.4 nodeOrgs.ca 配置

同 nodeOrgs

## 7 密码材料生成物目录结构

密码材料生成工具默认生成 consenterOrganizations, nodeOrganizations, consenterOrganizations.ca, nodeOrganizations.ca 4个子目录。其中 consenterOrganizations, nodeOrganizations 用于测试阶段，consenterOrganizations.ca, nodeOrganizations.ca 用于正式环境。

本章节主要描述密码材料生成工具生成物所约束的目录结构，

以节点的某一组织为例，如表6-1所示。

**表 6-1 组织的目录结构**

| 目录名称 | 目录说明 |
|---|---|
| ca | 根 CA 证书和密钥，后缀为.pem 的是证书，_sk 后缀的是密钥 |
| msp | MSP 的配置，参考后面的表格 |
| consenters | consenter 节点的配置 |
| tls_ca | TLS/SSL 的中间 CA 证书和密钥，后缀为.pem 的是证书，_sk 后缀的是密钥 |
| users | 默认生成的用户配置，一般会包含 1 个管理员和 1 个普通成员 |

MSP 目录的说明，如表 6-2 所示。

**表 6-2 MSP 的目录结构**

| 目录文件名称 | 目录文件说明 |
|---|---|
| admin_certs | MSP 的管理员证书 |
| ca_certs | MSP 的根 CA 证书 |
| keystore | 签名密钥 |
| sign_certs | 节点的签名证书 |
| tls_ca_certs | TLS/SSL 的根 CA 证书 |

在每个节点或者用户除了 MSP 目录，还有 tls 目录，用来进行 TLS/SSL 连接的配置。如表 6-3 所示。

**表 6-3 TLS 的目录结构**

| 文件名称 | 文件说明 |
|---|---|
| ca.crt | 可信的根 CA 证书 |
| server.crt | 用来进行 TLS/SSL 连接的证书 |
| server.key | 用来进行 TLS/SSL 连接的密钥 |

### 7.1 consenterOrganizations 目录

consenterOrganizations 目录存放配置文件中 consenterOrgs 声明的 consenter 节点所属组织的密码材料。

#### 7.1.1 组织目录

组织目录是 consenterOrganizations 的子目录，名字使用 consenterOrgs 各组织的 domain 配置值。

域名目录存放配置文件中 consenterOrgs 声明的各个组织域名对应的密码材料。

##### 7.1.1.1 ca 目录

ca 目录存放该组织域名的根证书和私钥，证书Subject和DN受配置项6.1.4 ca 配置项控制，组织内的实体将基于该根证书作为证书根。

##### 7.1.1.2 consenters 目录

consenters 目录存放该组织所有 consenter 节点的密码材料。

consenter 节点文件夹名字由 6.1.3 Specs 和 6.1.5 Template 配置后得到的证书 DN。

###### 7.1.1.2.1 msp 目录

msp 目录拷贝 7.1.1.3 的 msp 目录到本目录，并增加该 consenter 节点的私钥和证书。

###### 7.1.1.2.1.1 admin_certs 目录

admin_certs 目录存放该组织管理员的身份验证证书。Consenter 将基于这些证书来认证交易签名签署者是否为管理员身份。

命名格式为 Admin@{domain}-cert.pem。该证书与 7.1.1.5.1.1 中的管理员证书一致。

###### 7.1.1.2.1.2 ca_certs 目录

ca_certs 目录存放该组织的根证书。同 ca 目录下的文件。

命名格式为{CA_DN}-cert.pem，其中 CA_DN 为 6.1.4 中配置的 CA 证书的 DN。

###### 7.1.1.2.1.3 keystore 目录

keystore 目录存放该节点的身份私钥，用于签名。

名字格式为{ski}_sk，ski 为 CSP 模块中 IKey.ski()返回的字符串值。

###### 7.1.1.2.1.4 sign_certs 目录

sign_certs 目录存放验证本节点签名的证书，被组织的根证书签名。

命名格式为{commonName}@{Domain}-cert.pem。commonName由6.1.3.2 commonName配置项配置。

###### 7.1.1.2.1.5 tls_ca_certs 目录

tls_ca_certs 目录存放该组织 TLS/SSL 连接用的证书。

命名格式为 tls{CA_CERT}，其中 CA_CERT 为 7.1.1.2.1.2 的证书名。

###### 7.1.1.2.2 tls 目录

tls 目录存放该组织 TLS/SSL 连接相关的证书与私钥。里面包含 3 个文件：

- server.key：该节点的身份私钥，用于签名。
- server.crt：用来进行 TLS/SSL 连接的证书，被组织的根证书签名。
- ca.crt：组织的根证书

#### 7.1.1.3 msp 目录

msp 目录存放代表该组织的身份信息。

##### 7.1.1.3.1 admin_certs 目录

同 7.1.1.2.1.1。

##### 7.1.1.3.2 ca_certs 目录

同 7.1.1.2.1.2。

##### 7.1.1.3.3 tls_ca_certs 目录

同 7.1.1.2.1.3。

#### 7.1.1.4 tls_ca 目录

tlsca 目录包含该节点的 TLS/SSL CA 证书及 TLS/SSL CA 证书对应私钥。共两个文件。

- CA 证书：名字格式为 tls{CA 证书 DN}-cert.pem，如 tlsca.example.com-cert.pem，其中 ca.example.com 为 CA 证书 DN。
- CA 私钥：名字格式为{ski}_sk，ski 为 CSP 模块中 IKey.ski()返回的字符串值。

#### 7.1.1.5 users 目录

users 目录存放该组织的用户的实体。对于 consenter 节点来说，一般会包含 1 个管理员和一个普通成员。

users 子目录为各用户密码材料文件夹，子目录文件夹名的格式为{Username}@{domain}，管理员对应{Username}为Admin。

##### 7.1.1.5.1 msp 目录

msp 目录会拷贝 7.1.1.3 的 msp 目录到本目录，并增加该 user 的私钥和证书。

###### 7.1.1.5.1.1 admin_certs 目录

同 7.1.1.3.1。

###### 7.1.1.5.1.2 ca_certs 目录

同 7.1.1.3.2。

###### 7.1.1.5.1.3 keystore 目录

keystore 目录存放该用户的身份私钥，用于签名。

名字格式为{ski}_sk，ski 为 CSP 模块中 IKey.ski()返回的字符串值。

###### 7.1.1.5.1.4 sign_certs 目录

sign_certs 目录存放该用户的身份证书，被组织的根证书签名。

命名格式为{Username}@{Domain}-cert.pem。该证书由 concenter 节点 CA 证书签发。

#### 7.1.1.5.1.5 tls_ca_certs 目录

同 4.1.1.3.3。

#### 7.1.1.5.2 tls 目录

tls 目录存放该用户的 TLS/SSL 连接所需证书。里面包含 3 个文件：

- client.key：用户的身份私钥，用于签名。
- server.crt：用来进行 TLS/SSL 连接的证书，被组织的根证书签名。
- ca.crt：组织的根证书。

### 7.2 nodeOrganizations 目录

nodeOrganizations目录存放配置文件中 nodeOrgs 声明的 node 节点所属组织的密码材料。

#### 7.2.1 组织目录

组织目录是 nodeOrganizations 的子目录，名字使用 nodeOrgs各组织的domain配置值。
组织目录存放配置文件中 nodeOrgs 声明的各个组织域名对应的密码材料。

#### 7.2.1.1 ca 目录

ca 目录存放该组织域名的根证书和私钥，证书 Subject 和 DN 受配置项 6.1.4 ca 配置项控制，组织内的实体将基于该根证书作为证书根。

#### 7.2.1.2 msp 目录

msp 目录存放代表该组织的身份信息。

#### 7.2.1.2.1 admin_certs 目录

admin_certs 目录存放该组织管理员的身份验证证书。Consenter 将基于这些证书来认证交易签名签署者是否为管理员身份。
命名格式为 Admin@{domain}-cert.pem。该证书与 7.2.1.5.1.1 中的管理员证书一致。

#### 7.2.1.2.2 ca_certs 目录

ca_certs 目录存放该组织的根证书。同 ca 目录下的文件。
命名格式为{CA_DN}-cert.pem，其中 CA_DN 为 6.2.4 中配置的 CA 证书的 DN。

#### 7.2.1.2.3 tls_ca_certs 目录

tls_ca_certs 目录存放该组织 TLS/SSL 连接用的 TLS 证书。
命名格式为 tls{CA_CERT}，其中 CA_CERT 为 7.2.1.2.2 的证书名。

#### 7.2.1.3 nodes 目录

nodes 目录存放该组织节点所有 node 节点的密码材料。
nodes 节点文件夹名字由 6.2.3 Specs 和 6.2.5 Template 配置后得到的证书 DN。

#### 7.2.1.3.1 msp 目录

msp 目录会拷贝 7.2.1.2 的 msp 目录到本目录，并增加该 user 的私钥和证书。

#### 7.2.1.3.1.1 admin_certs 目录

同 7.2.1.2.1

#### 7.2.1.3.1.2 cacerts 目录

同 7.2.1.2.2

#### 7.2.1.3.1.3 keystore 目录

keystore 目录存放该节点的身份私钥，用于签名。
名字格式为{ski}_sk，ski 为 CSP 模块中 IKey.ski()返回的字符串值

#### 7.2.1.3.1.4 sign_certs 目录

sign_certs 目录存放验证本节点签名的证书，被组织的根证书签名。
命名格式为{commonName}@{Domain}-cert.pem。该证书由 node 节点 MSP 的根 CA 证书签发。

#### 7.2.1.3.1.5 tls_ca_certs 目录

同 7.2.1.2.3

### 7.2.1.3.2 tls 目录

tls 目录存放该组织 TLS/SSL 连接相关的证书与私钥。里面包含 3 个文件：

- server.key：该节点的身份私钥，用于签名。
- server.crt：用于通信安全的证书，被组织的根证书签名。
- ca.crt：组织的根证书

### 7.2.1.4 tls_ca 目录

tlsca 目录包含该节点的 TLS/SSL CA 证书及 TLS/SSL CA 证书对应私钥。共两个文件。

- CA 证书：名字格式为 tls{CA 证书 DN}-cert.pem，如 tlsca.example.com-cert.pem，其中 ca.example.com 为 CA 证书 DN。
- CA 私钥：名字格式为{ski}_sk，ski 为 CSP 模块中 IKey.ski()返回的字符串值。

### 7.2.1.5 users 目录

users 目录存放该组织的用户的实体。与consenter节点不一样，node节点，有一个Admin用户和0个或多个普通User用户。

users 子目录为各用户密码材料文件夹，子目录文件夹名的格式为{Username}@{domain}。
管理员对应{Username}为Admin，用户对应的{Username}为User{num}，num从1开始递增。

#### 7.2.1.5.1 msp 目录

msp 目录会拷贝 7.2.1.2 的 msp 目录到本目录，并增加该 user 的私钥和证书。

#### 7.2.1.5.1.1 admin_certs 目录

同 7.2.1.2.1。

#### 7.2.1.5.1.2 ca_certs 目录

同 7.2.1.2.2。

#### 7.2.1.5.1.3 keystore 目录

keystore 目录存放该用户的身份私钥，用于签名。
名字格式为{ski}_sk，ski 为 CSP 模块中 IKey.ski()返回的字符串值。

#### 7.2.1.5.1.4 sign_certs 目录

signcerts 目录存放该用户的身份证书，被组织的根证书签名。
命名格式为{UserName}@{Domain}-cert.pem。

#### 7.2.1.5.1.5 tls_ca_certs 目录

同 7.2.1.2.3。

#### 7.2.1.5.2 tls 目录

tls 目录存放该用户的 TLS/SSL 连接所需证书。里面包含 3 个文件：

- client.key：用户的身份私钥，用于签名。
- server.crt： 用来进行 TLS/SSL 连接的证书，被组织的根证书签名。
- ca.crt：组织的根证书。

### 7.3 consenterOrganizations.ca 目录

同 consenterOrganizations 目录。

### 7.4 nodeOrganizations.ca 目录

同 nodeOrganizations 目录。

## 8 CSR 配置文件规范

本章节描述了密码材料生成工具生成 CSR 文件，所依赖的配置文件字段的内容和约束。

### 8.1 cn 配置

CA签名请求文件中的通用名（common name）域。

### 8.2 keyrequest

#### 8.2.1 algo 配置

生成密钥所使用的算法。

#### 8.2.2 size 配置

密钥大小。

### 8.3 serialnumber 配置

CA签名请求文件中的序列号域，会成为DN的一部分。

### 8.4 names 配置

证书的 Subject对象，至少包含一个“C”，“L”，“O”，“OU”，“ST”字段，或者它们的任意组合。

#### 8.4.1 C 配置

country的简写，所在的国家，以国际标准化组织（ISO）的两字母格式表示。

#### 8.4.2 L 配置

locality的简写，所在的地区或直辖市。

#### 8.4.3 O 配置

organization的简写，所在的组织。

#### 8.4.4 OU 配置

organizational unit的简写，所在的组织机构单位。

#### 8.4.5 ST 配置

state的简写，所在的州或者省。

### 8.5 hosts 配置

CA签名请求文件中的主机名，默认为本地主机名称，可以有多个主机名。

### 8.6 ca 配置

#### 8.6.1 expiry 配置

超时时间

#### 8.6.2 pathlength 配置

允许产生的中间证书的深度

## 9 密码材料生成工具与 CSP

密码材料生成工具通过上层提供的 CSP 实例调用底层 CSP 接口去生成所需的密码材料，上层的 CSP 可根据配置文件更改不同的实现，实现 CSP 模块的可插拔支持。

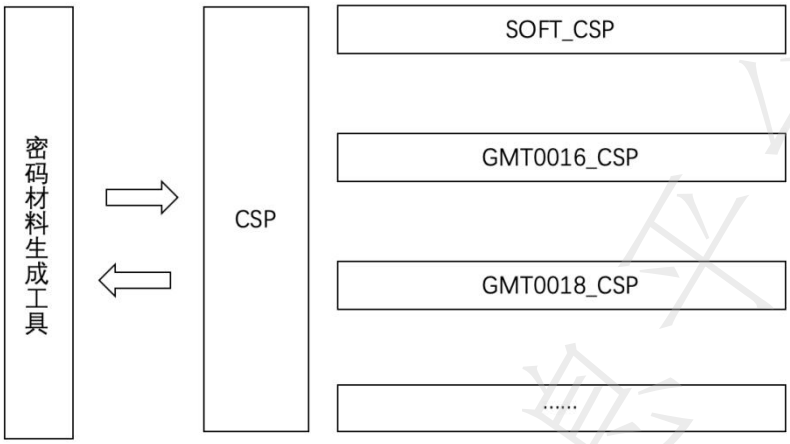


图8-1 密码材料生成工具与 CSP 的调用关系

## 10 密码材料生成工具安全要求

- 应使用区块链内置 CSP 模块进行密码生成和签名操作。
- 密码学安全性由区块链 CSP 模块密码学安全性保证。
- 生成的密码材料应使用国密算法，证书内容应符合国密证书标准。