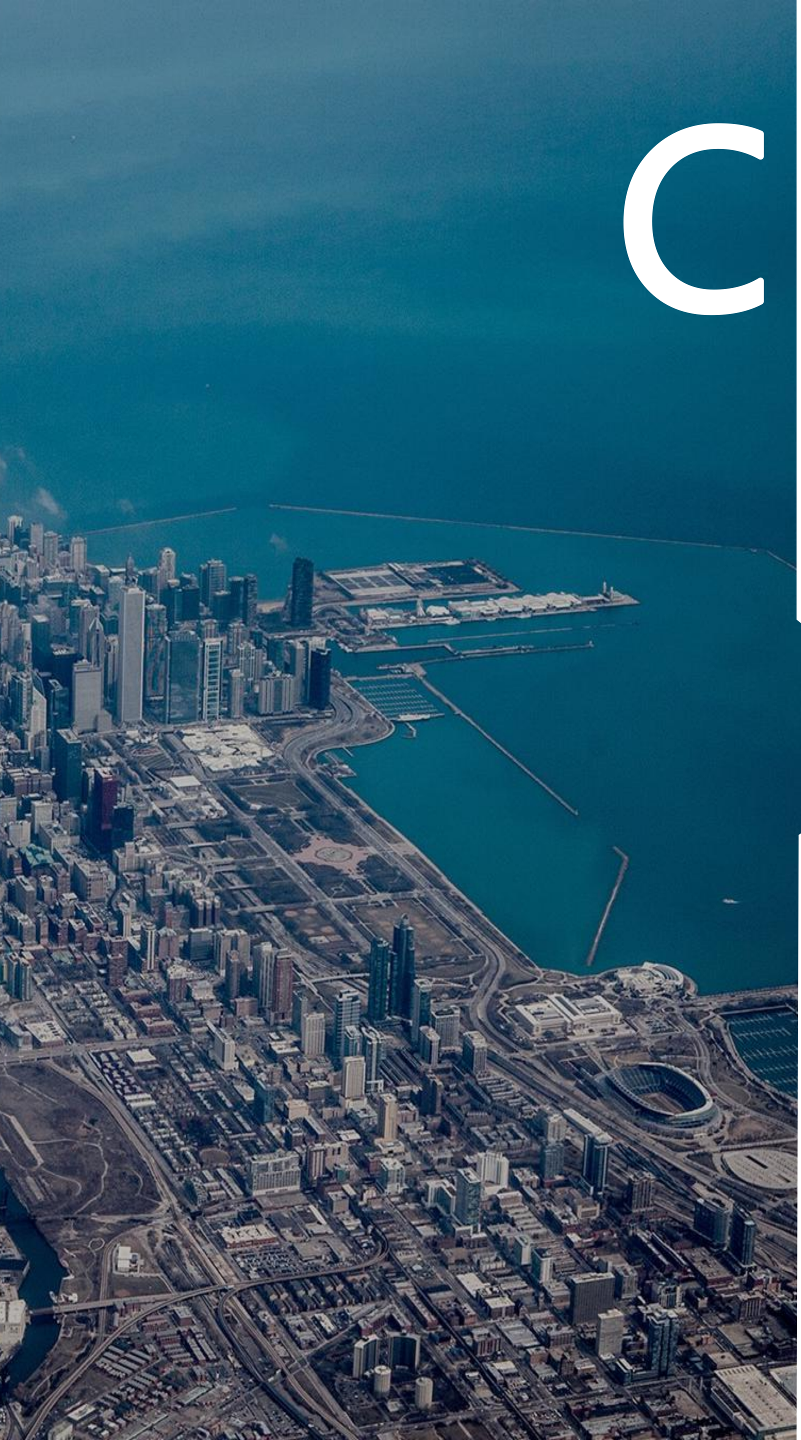
区块链技术与应用

华南理工大学　　许可　　kexu@scut.edu.cn

本课件主要内容来源于IBM

Unit 5 Fabric MSP and CA



Contents

1 Fabric CA Overview

2 PKI - X.509

3 MSP structure and usage

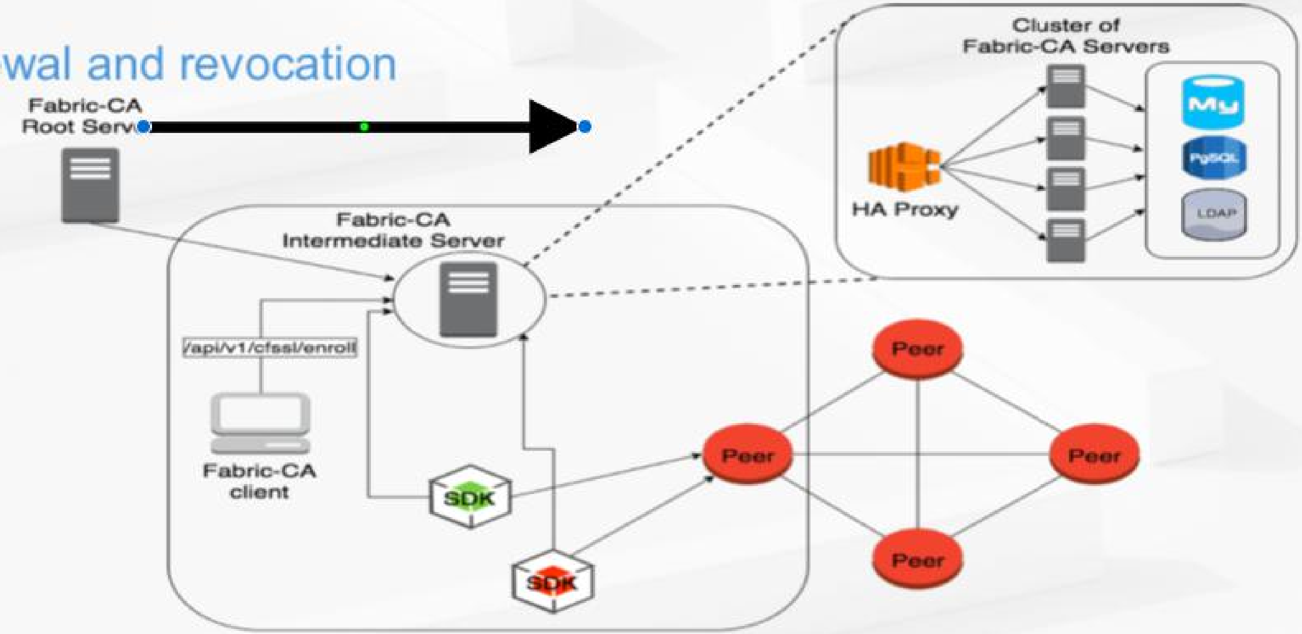
华南理工大学

Part 1

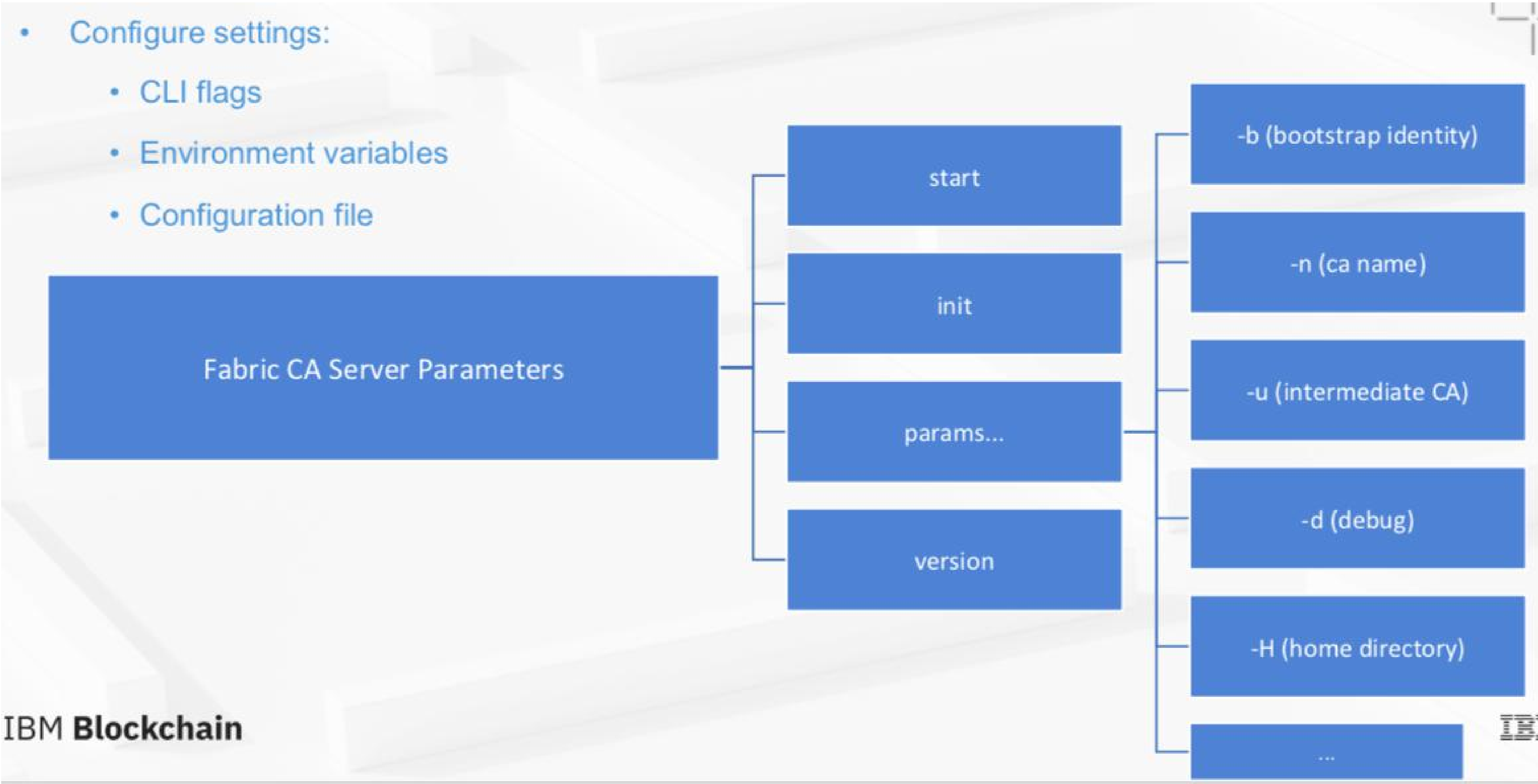
Fabric CA Overview

Hyperlegder Fabric CA

- Features:
  - Registration of identities
  - Enrollment Certs
  - Certificate renewal and revocation
- C/S
- Architecture



Fabric CA Server



- Configure settings:
  - CLI flags
  - Environment variables
  - Configuration file

Fabric CA Server Parameters

start

init

params...

version

-b (bootstrap identity)

-n (ca name)

-u (intermediate CA)

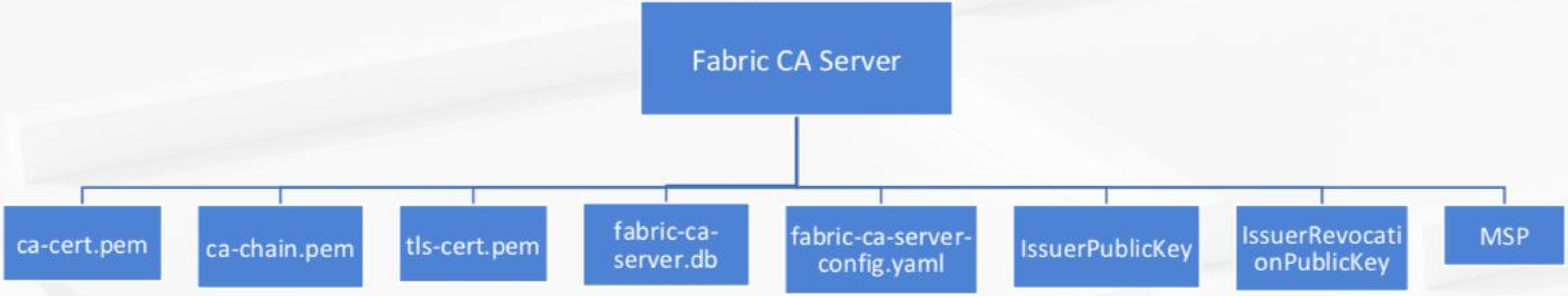
-d (debug)

-H (home directory)

...

IBM **Blockchain**

Fabric CA Server Init



Fabric CA Server

ca-cert.pem

ca-chain.pem

tls-cert.pem

fabric-ca-server.db

fabric-ca-server-config.yaml

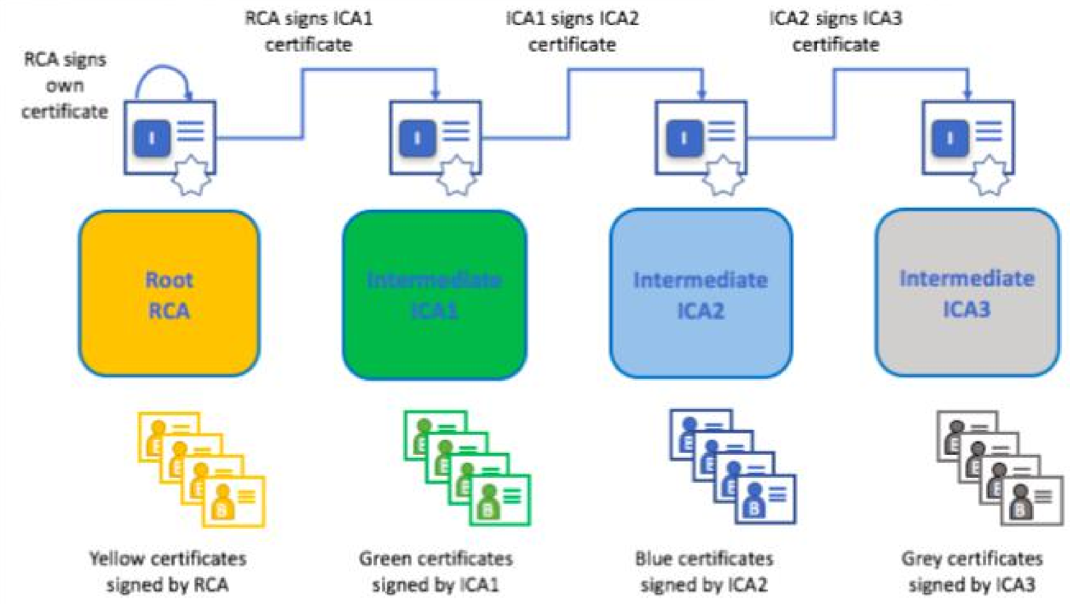
IssuerPublicKey

IssuerRevocationPublicKey

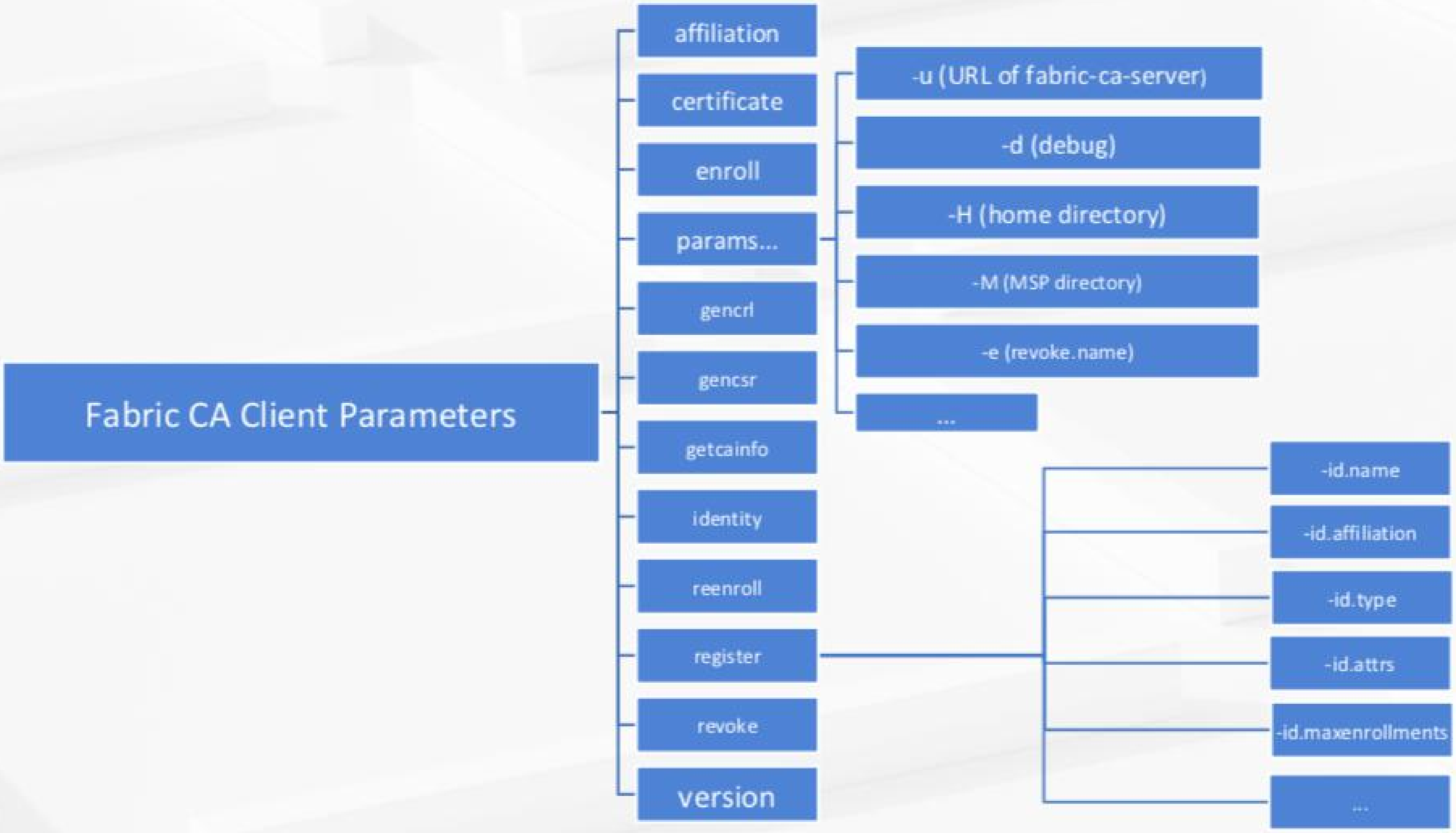
MSP

Intermedia CA

- Limit exposure of Root CA
- Across multiple organizations
- Enroll intermedia CA with Root CA
- Certificate Chain trust between Root CA and a set of Intermediate CA


RCA signs own certificate
RCA signs ICA1 certificate
ICA1 signs ICA2 certificate
ICA2 signs ICA3 certificate
Root RCA
Intermediate ICA1
Intermediate ICA2
Intermediate ICA3
Yellow certificates signed by RCA
Green certificates signed by ICA1
Blue certificates signed by ICA2
Grey certificates signed by ICA3

Fabric CA Client

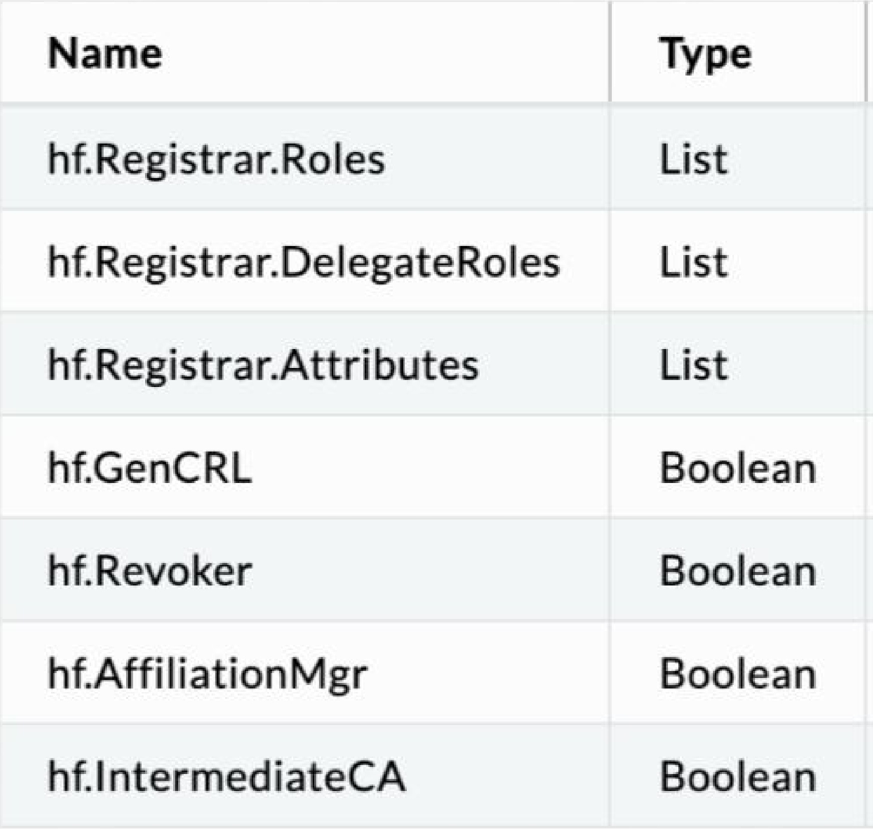


Fabric CA Client Parameters

- affiliation
- certificate
- enroll
- params...
  - -u (URL of fabric-ca-server)
  - -d (debug)
  - -H (home directory)
  - -M (MSP directory)
  - -e (revoke.name)
  - ...
- gencrl
- gencsr
- getcainfo
- identity
- reenroll
- register
  - -id.name
  - -id.affiliation
  - -id.type
  - -id.attrs
  - -id.maxenrollments
  - ...
- revoke
- version

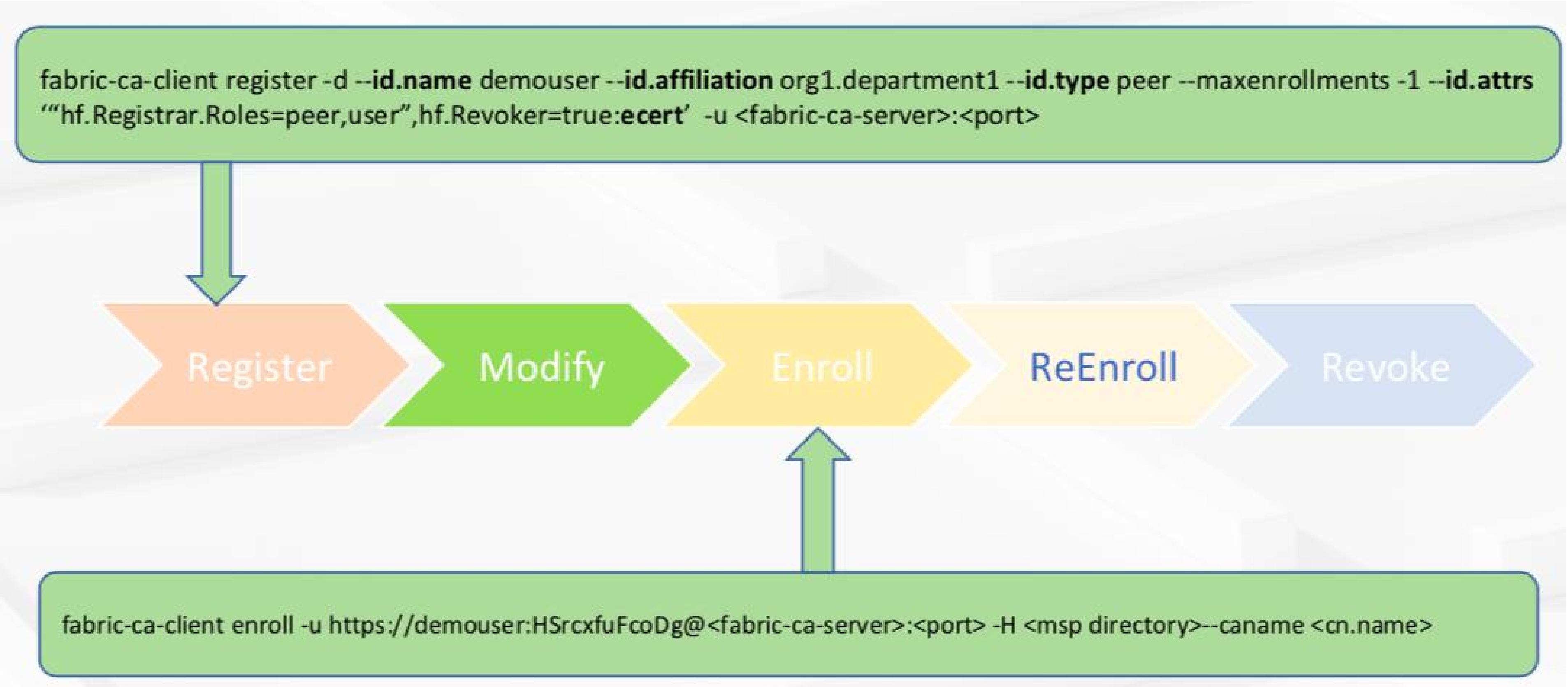
ABAC(Attribute-Based Access Control)

- Access control decision can be made by chaincode
  - Register with attributes - ‘**id.attrs**’
  - Enroll with attributes - ‘**enrollment.attrs**’
  - 3 default attributes in Ecert:
    - hf.EnrollmentID
    - hf.Type
    - hf.Affiliation
  - ‘:ecert’ to add attribute into Ecert



Name	Type
hf.Registrar.Roles	List
hf.Registrar.DelegateRoles	List
hf.Registrar.Attributes	List
hf.GenCRL	Boolean
hf.Revoker	Boolean
hf.AffiliationMgr	Boolean
hf.IntermediateCA	Boolean

Identity Lifecycle



```
fabric-ca-client register -d --id.name demouser --id.affiliation org1.department1 --id.type peer --maxenrollments -1 --id.attrs
‘“hf.Registrar.Roles=peer,user”,hf.Revoker=true:ecert’  -u <fabric-ca-server>:<port>
```

Register → Modify → Enroll → ReEnroll → Revoke

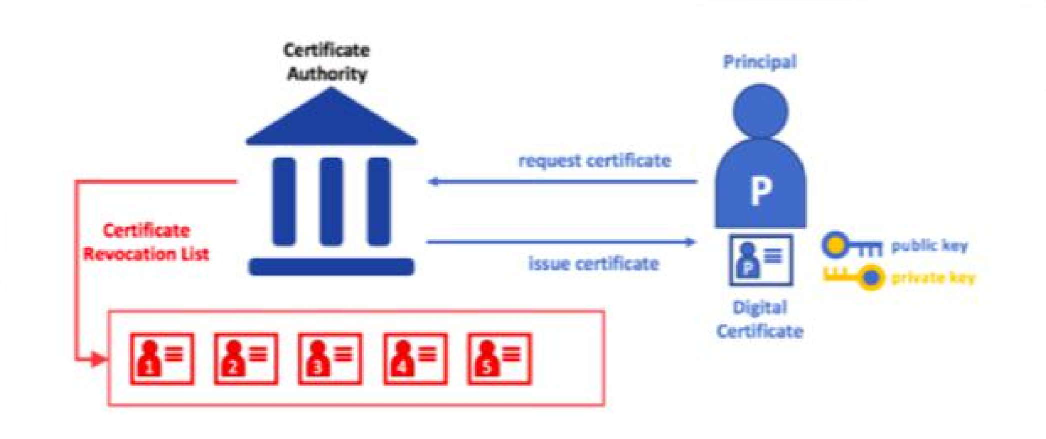
```
fabric-ca-client enroll -u https://demouser:HSrcxfuFcoDg@<fabric-ca-server>:<port> -H <msp directory>--caname <cn.name>
```

Part 2

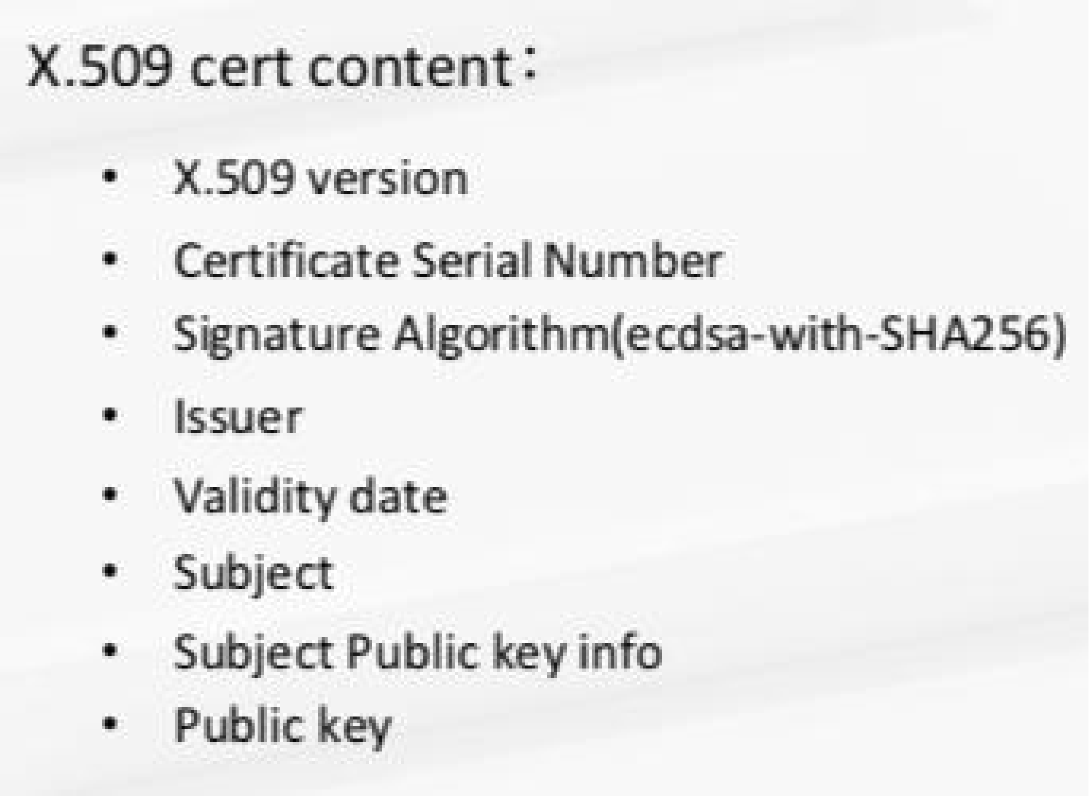
PKI - X.509

PKI

- PKI(Public Key Infrastructure)
-
    - Digital Certificates
    - Public and Private keys
    - Certificate Authorities
    - Certificate Revocation List



X.509 certificates by Fabric CA -1



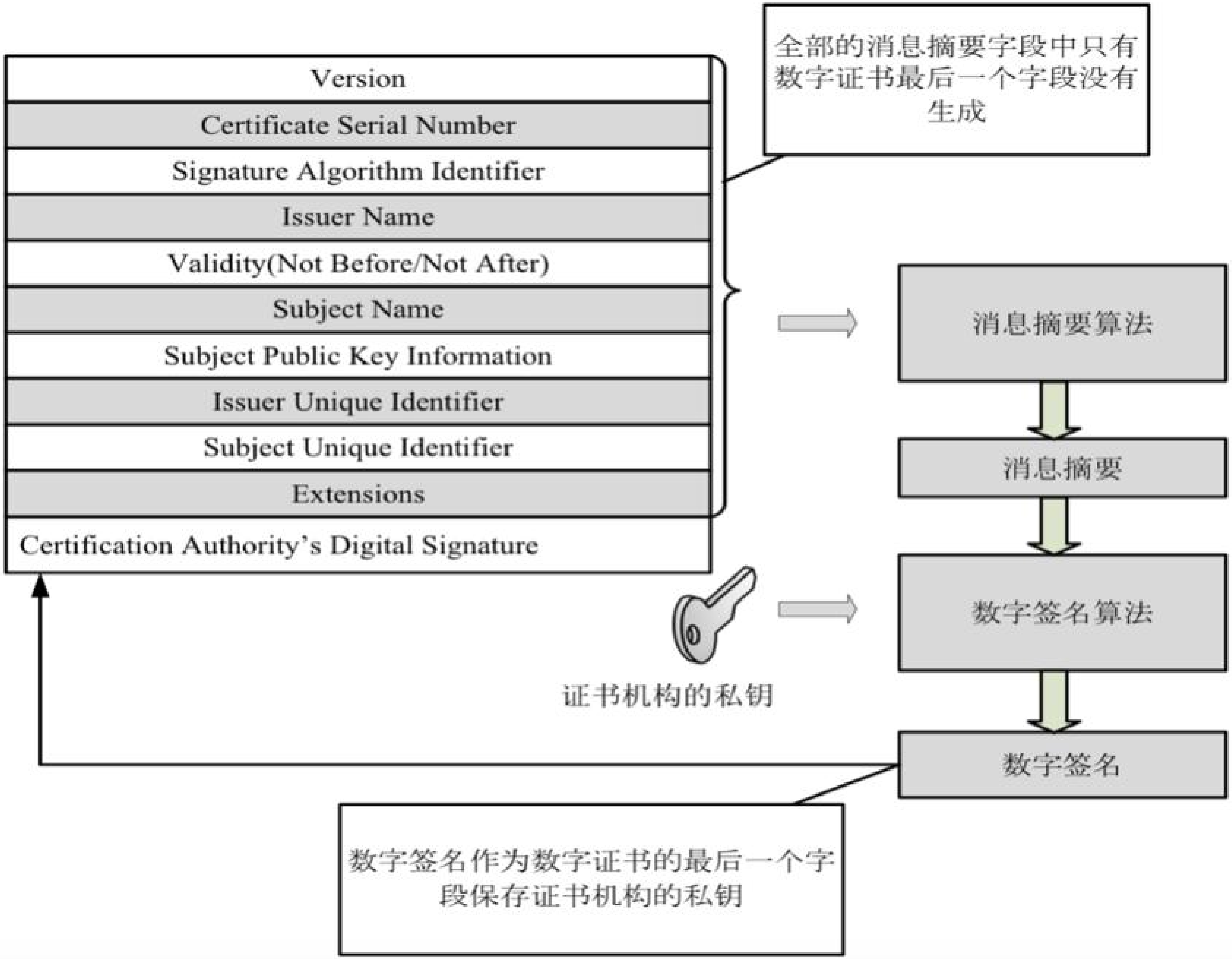
X.509 cert content：

- X.509 version
- Certificate Serial Number
- Signature Algorithm(ecdsa-with-SHA256)
- Issuer
- Validity date
- Subject
- Subject Public key info
- Public key

Three types of certifications

- ECert
- TLSCert
- TCert

Sign certifications



Version

Certificate Serial Number

Signature Algorithm Identifier

Issuer Name

Validity(Not Before/Not After)

Subject Name

Subject Public Key Information

Issuer Unique Identifier

Subject Unique Identifier

Extensions

Certification Authority's Digital Signature

全部的消息摘要字段中只有数字证书最后一个字段没有生成

消息摘要算法

消息摘要

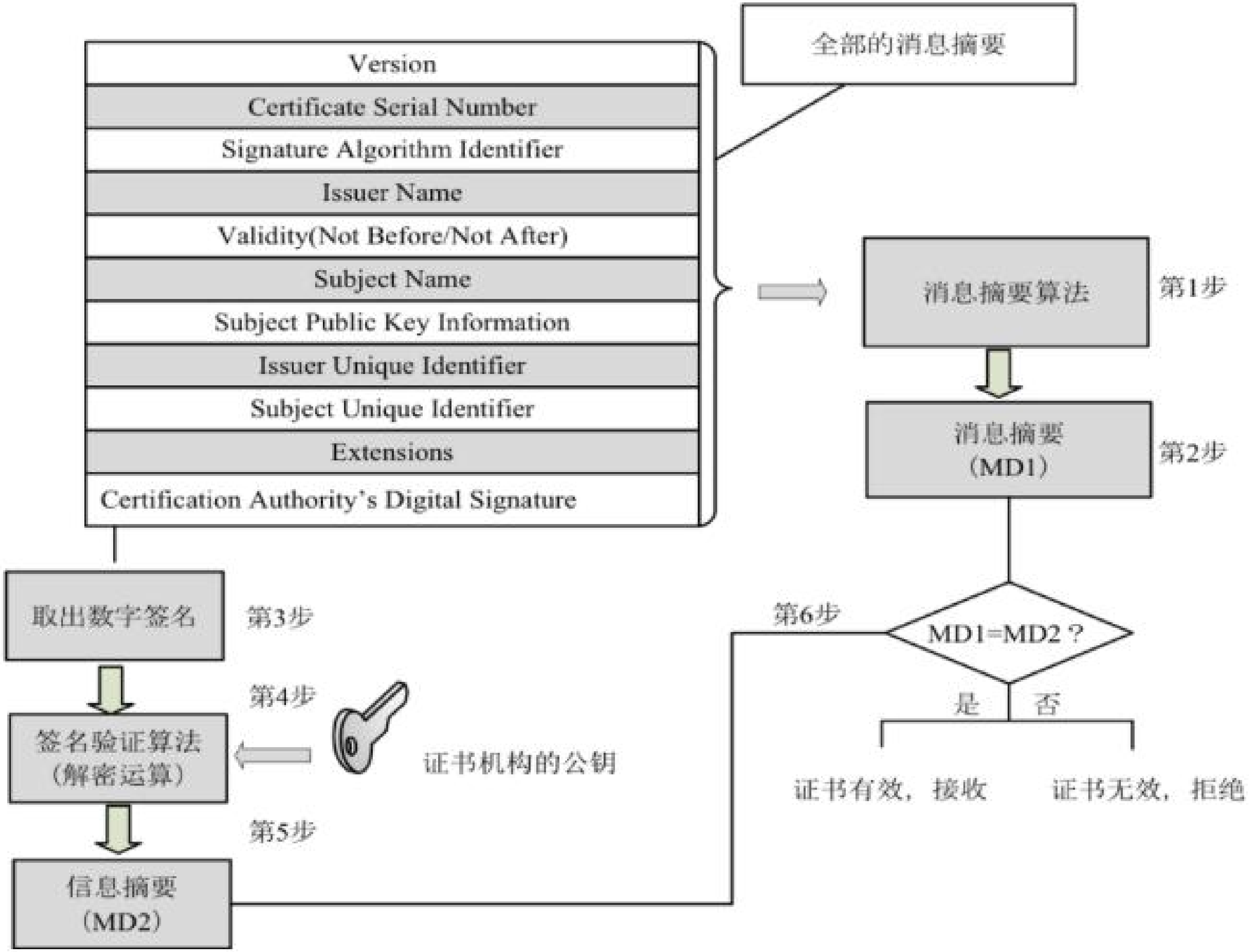
数字签名算法

数字签名

证书机构的私钥

数字签名作为数字证书的最后一个字段保存证书机构的私钥

Verify the certifications

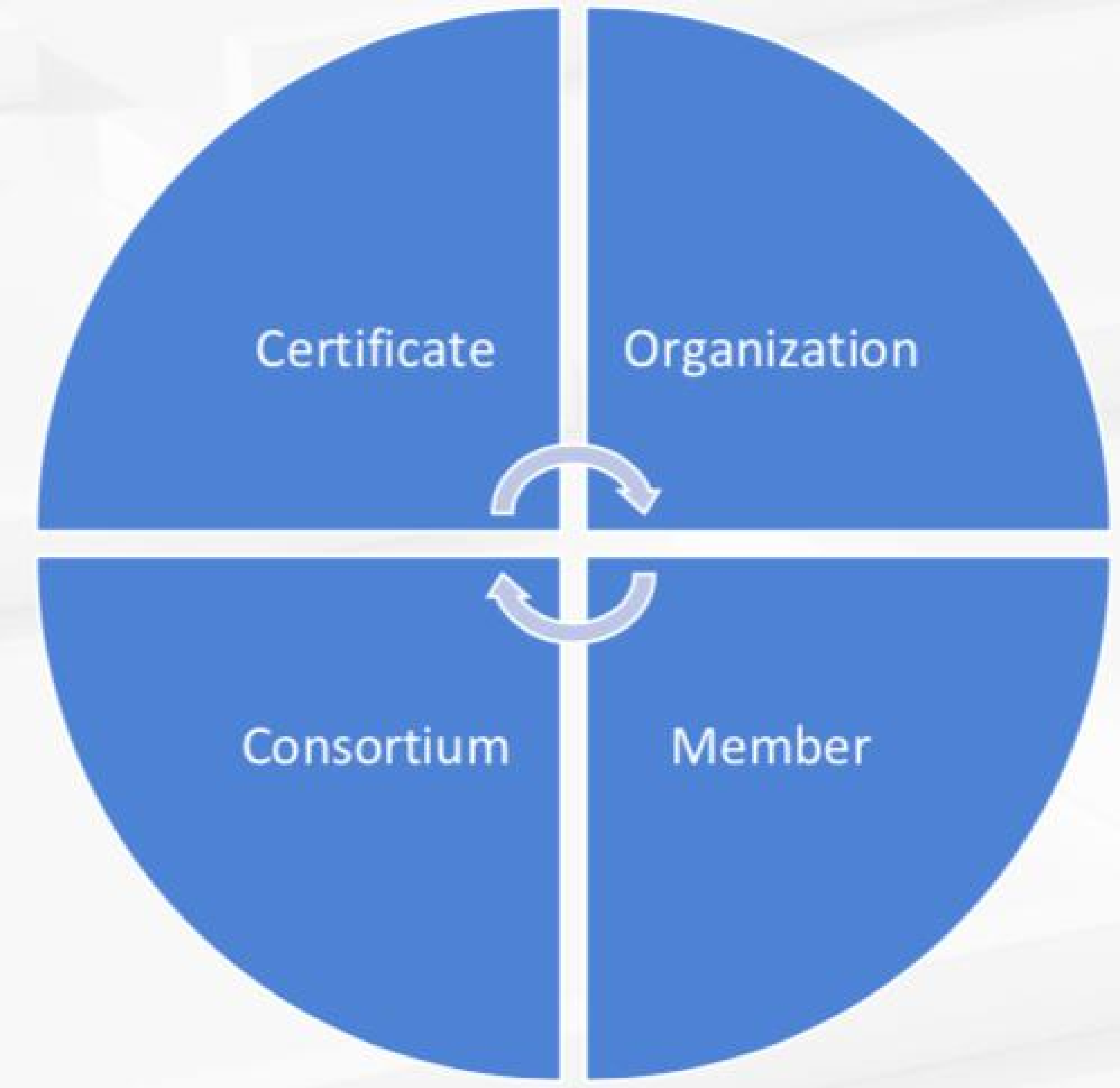


Version
Certificate Serial Number
Signature Algorithm Identifier
Issuer Name
Validity(Not Before/Not After)
Subject Name
Subject Public Key Information
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Certification Authority's Digital Signature

Part 3

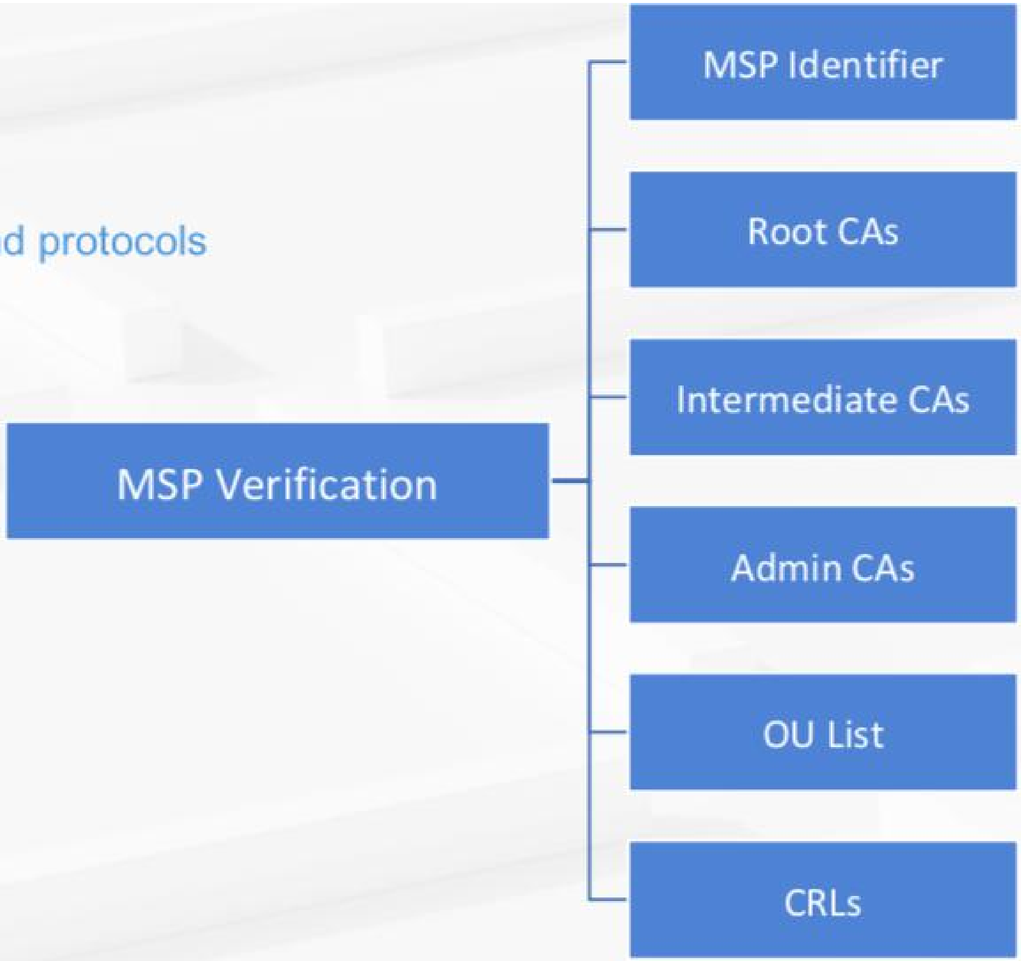
MSP structure and usage

Membership Service Provider



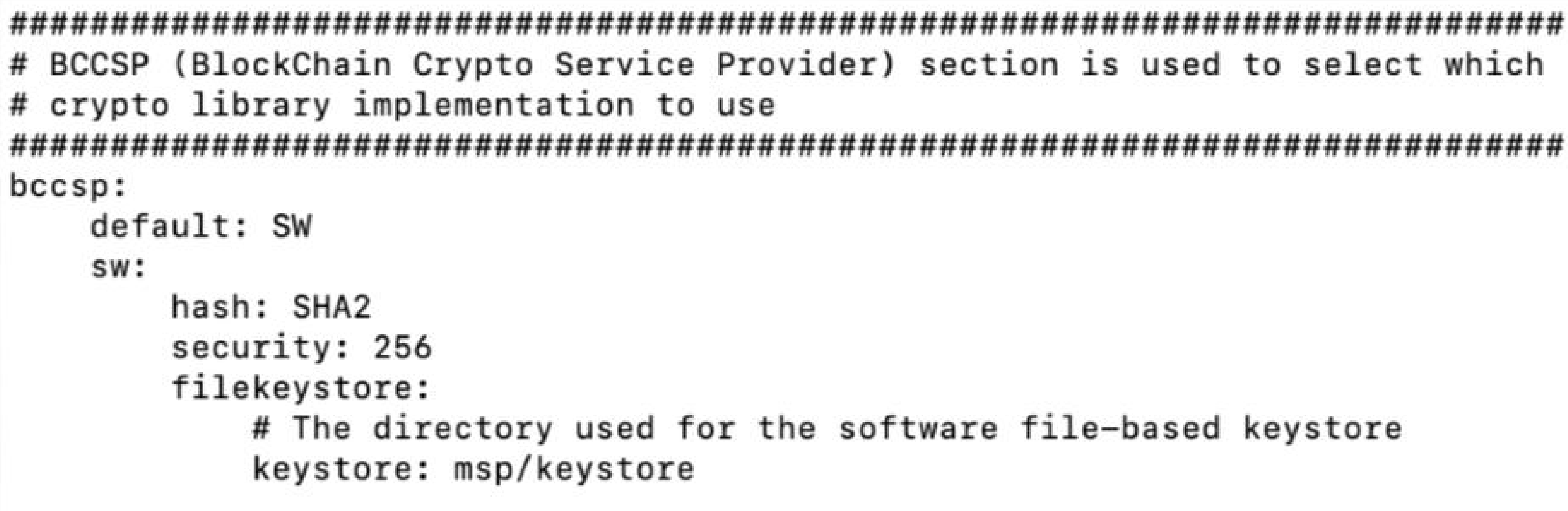
Membership Service Provider

- Abstracts all cryptographic mechanisms and protocols
- Provide credentials to clients and peers
  - clients - authenticate transaction
  - peers - endorsements
- 1-N MSP & MSP ID **unique**
- Fabric CA, OpenSSL, Cryptogen …



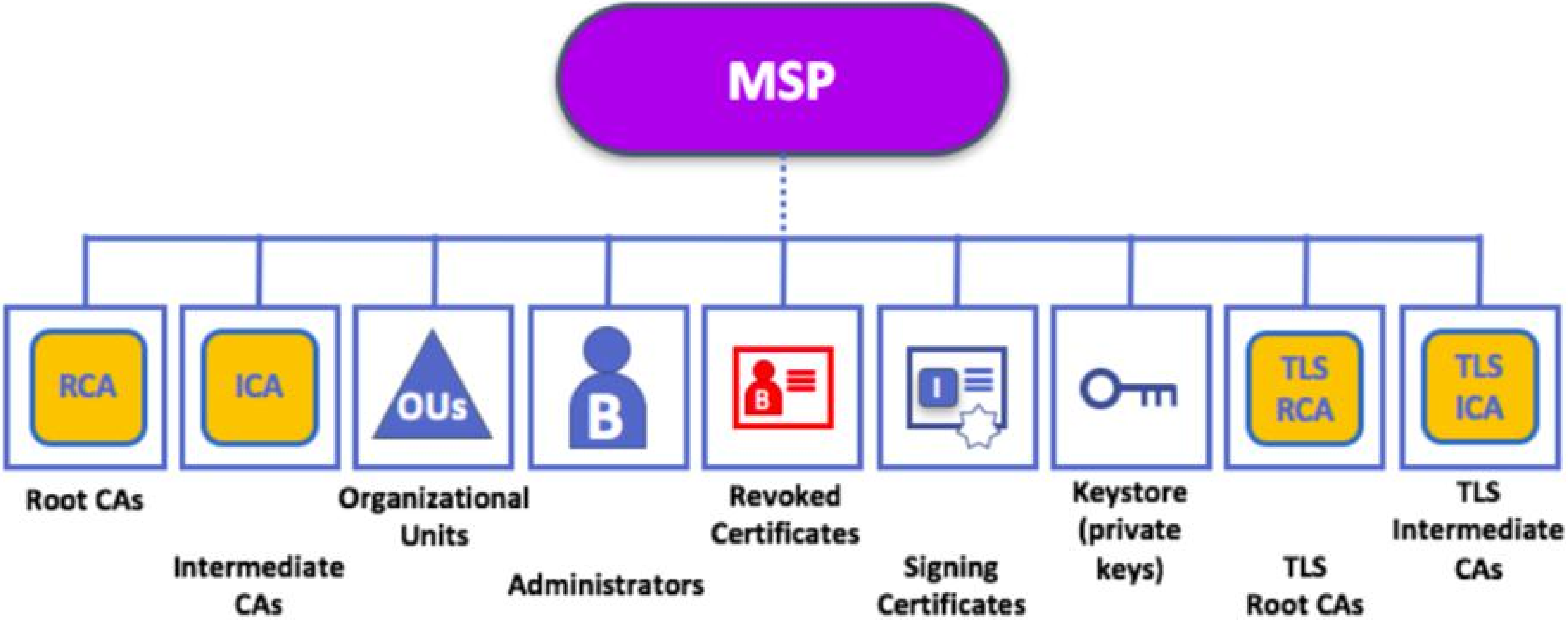
BCCSP

- Blockchain cryptographic service provider
- Implementation:
  - PKCS #11
  - SW

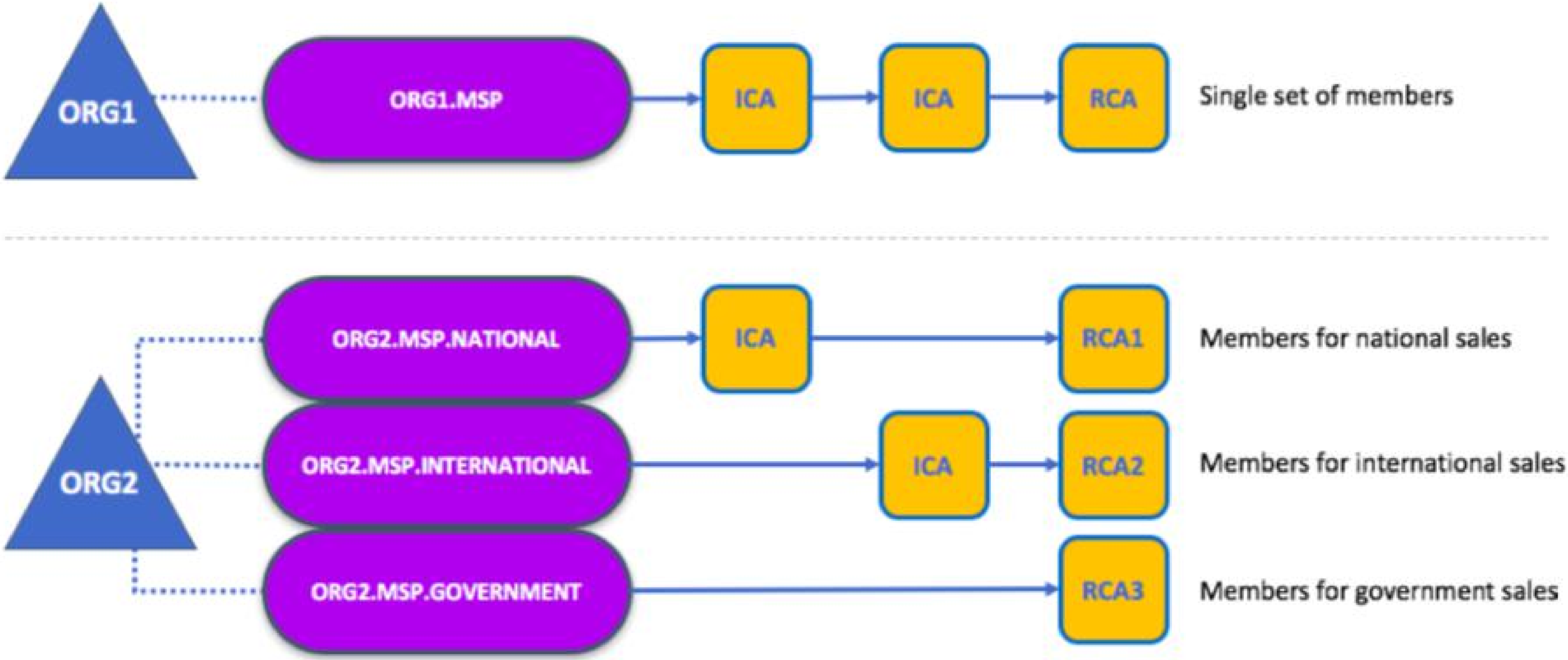


```
#############################################################################
# BCCSP (BlockChain Crypto Service Provider) section is used to select which
# crypto library implementation to use
#############################################################################
bccsp:
    default: SW
    sw:
        hash: SHA2
        security: 256
        filekeystore:
            # The directory used for the software file-based keystore
            keystore: msp/keystore
```

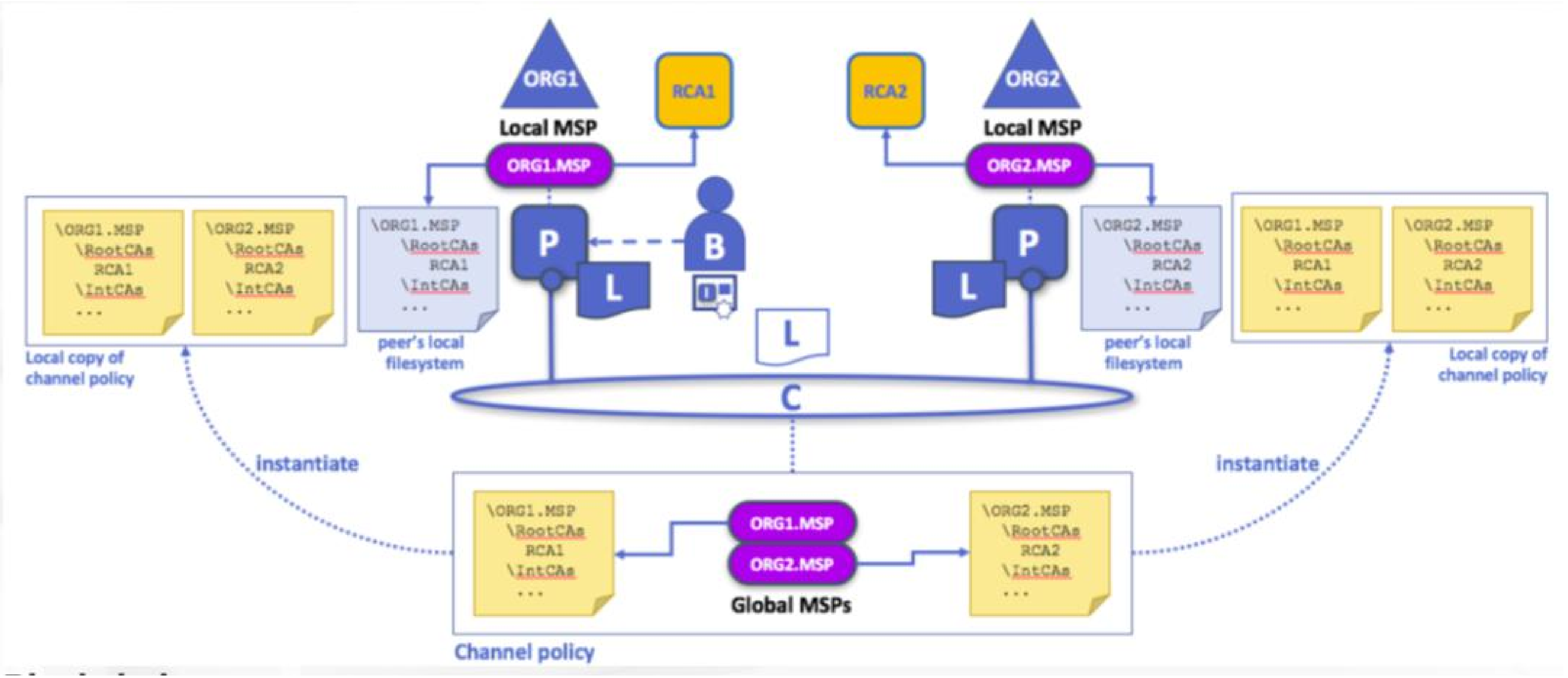
MSP Tree


MSP
RCA
ICA
OUs
B
TLS RCA
TLS ICA
Root CAs
Intermediate CAs
Organizational Units
Administrators
Revoked Certificates
Signing Certificates
Keystore (private keys)
TLS Root CAs
TLS Intermediate CAs

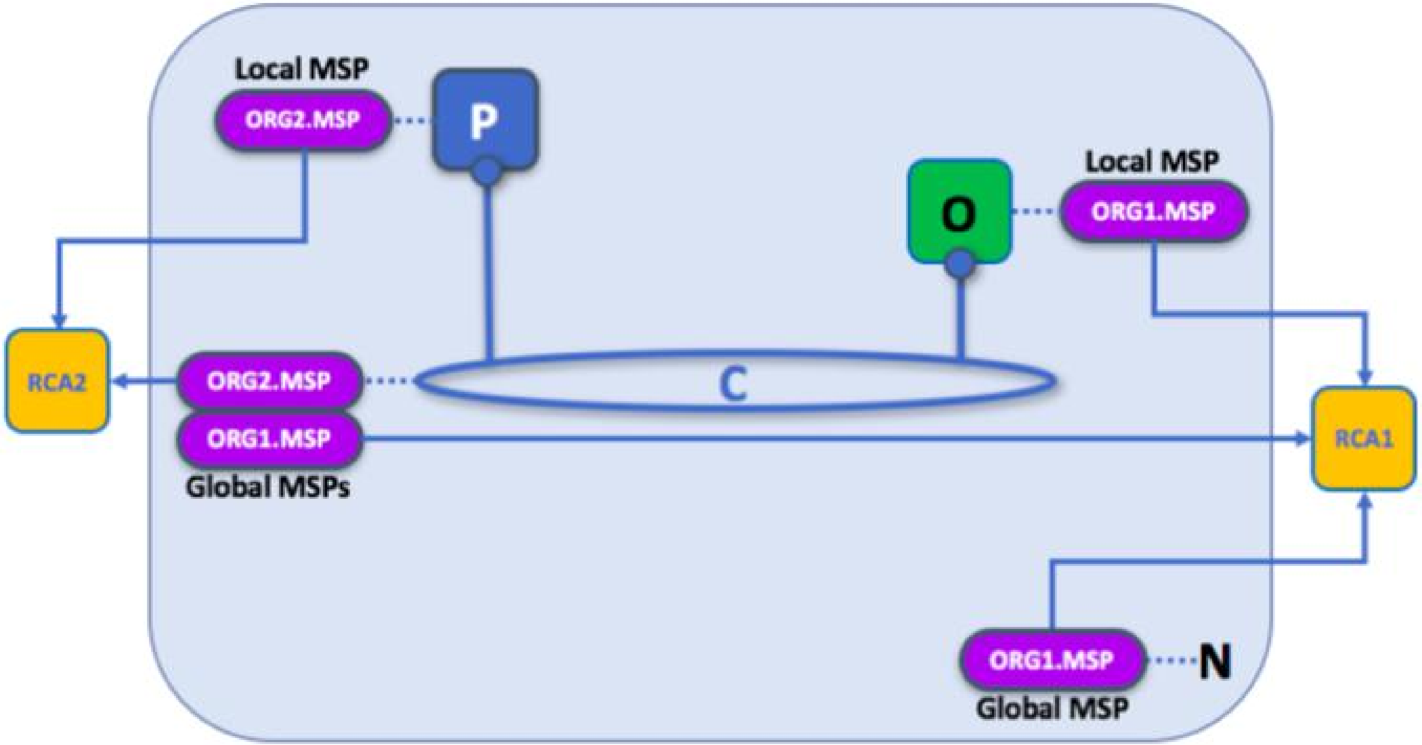
Organization - MSP



MSP in Channel



MSP Level



N	Blockchain Network
C	Channel
MSP	Membership Services Provider
P	Peer
O	Orderer
CA	Certificate Authority

Thanks!

华南理工大学