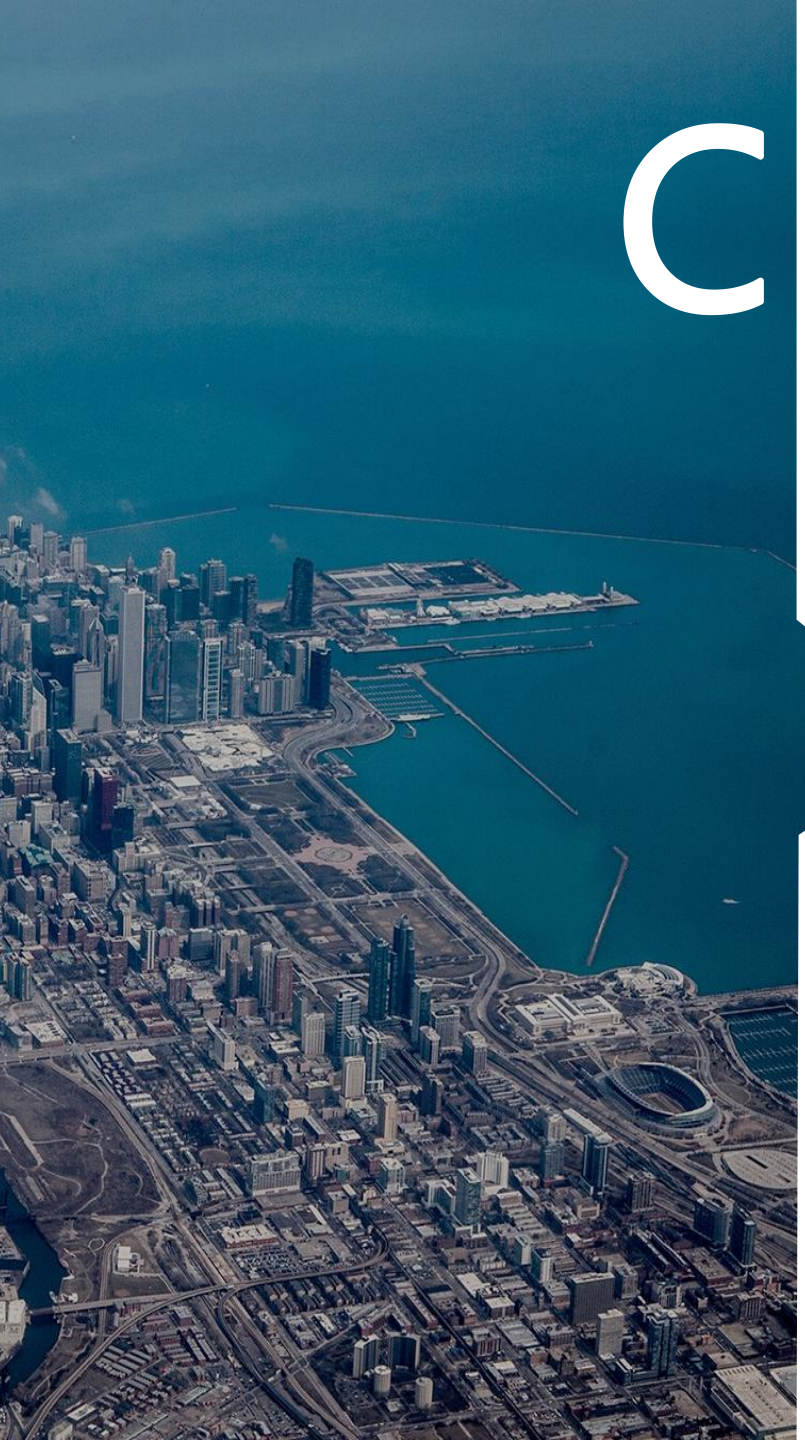
区块链技术与应用

华南理工大学　　许可　　kexu@scut.edu.cn

本课件主要内容来源于IBM

Unit 4 Fabric MSP and CA



Contents

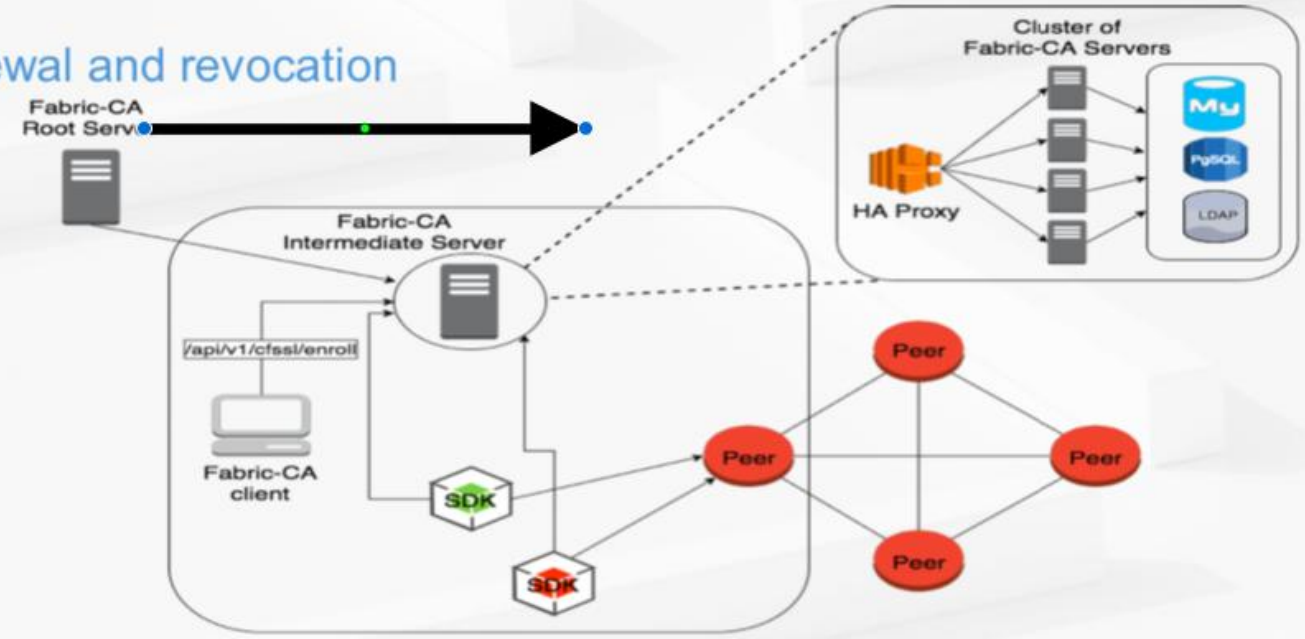
1. Fabric CA Overview
2. PKI - X.509
3. MSP structure and usage

Part 1

Fabric CA Overview

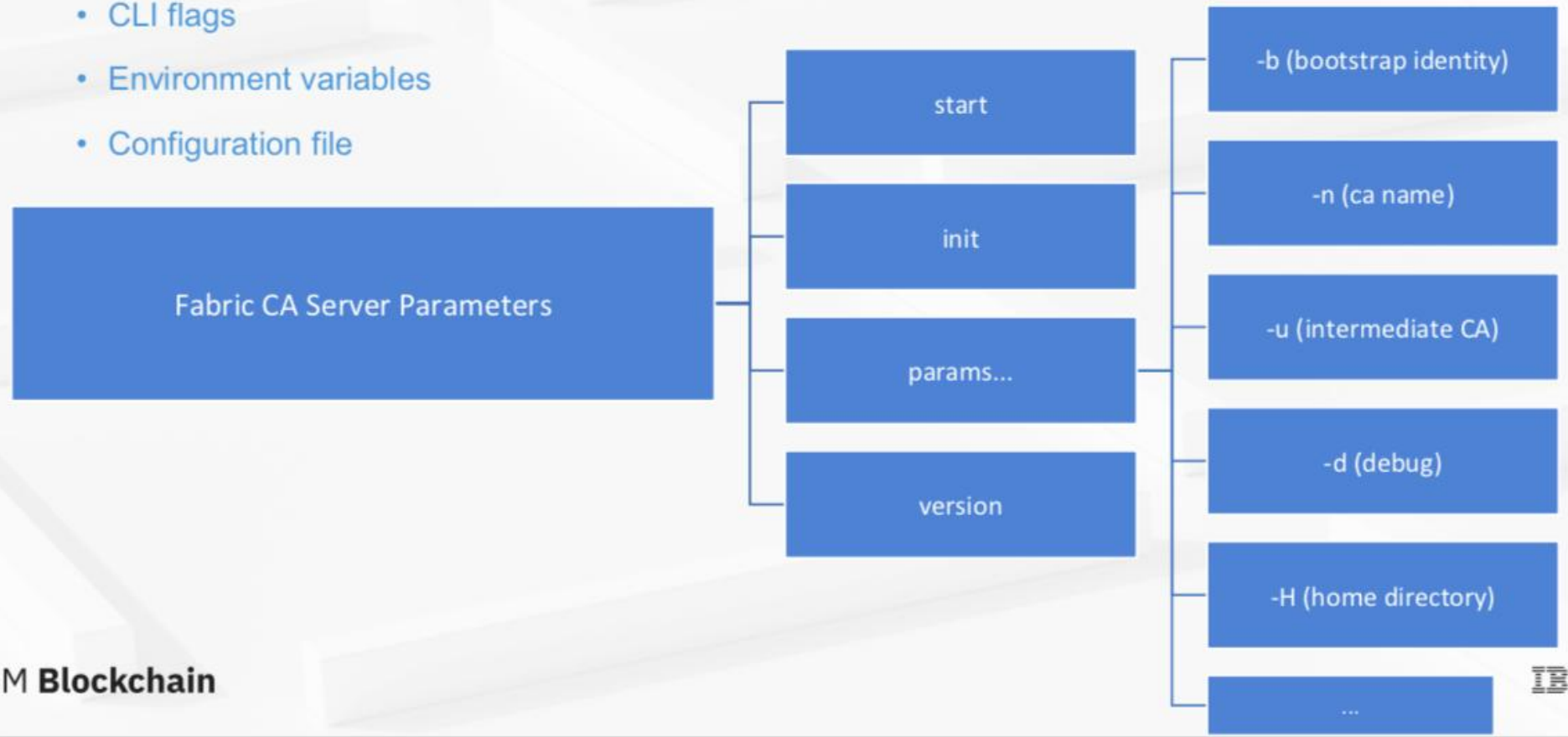
Hyperlegder Fabric CA

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

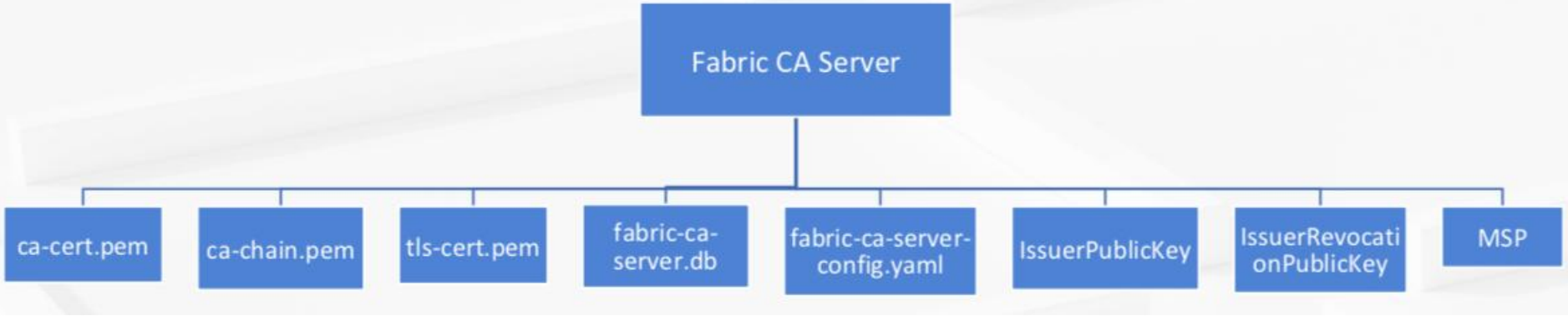


Fabric CA Server

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

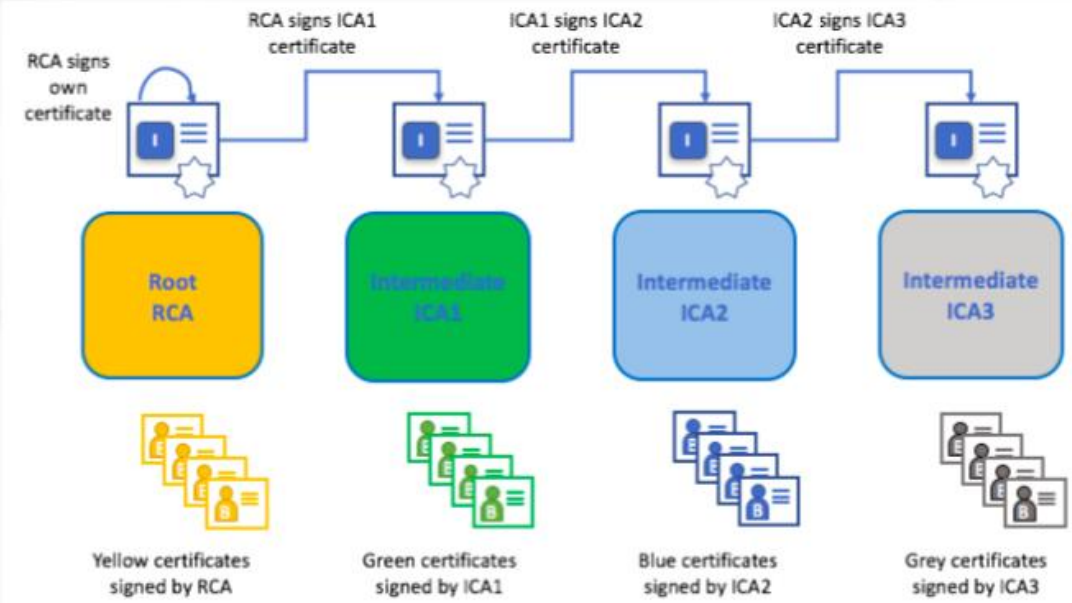


Fabric CA Server Init

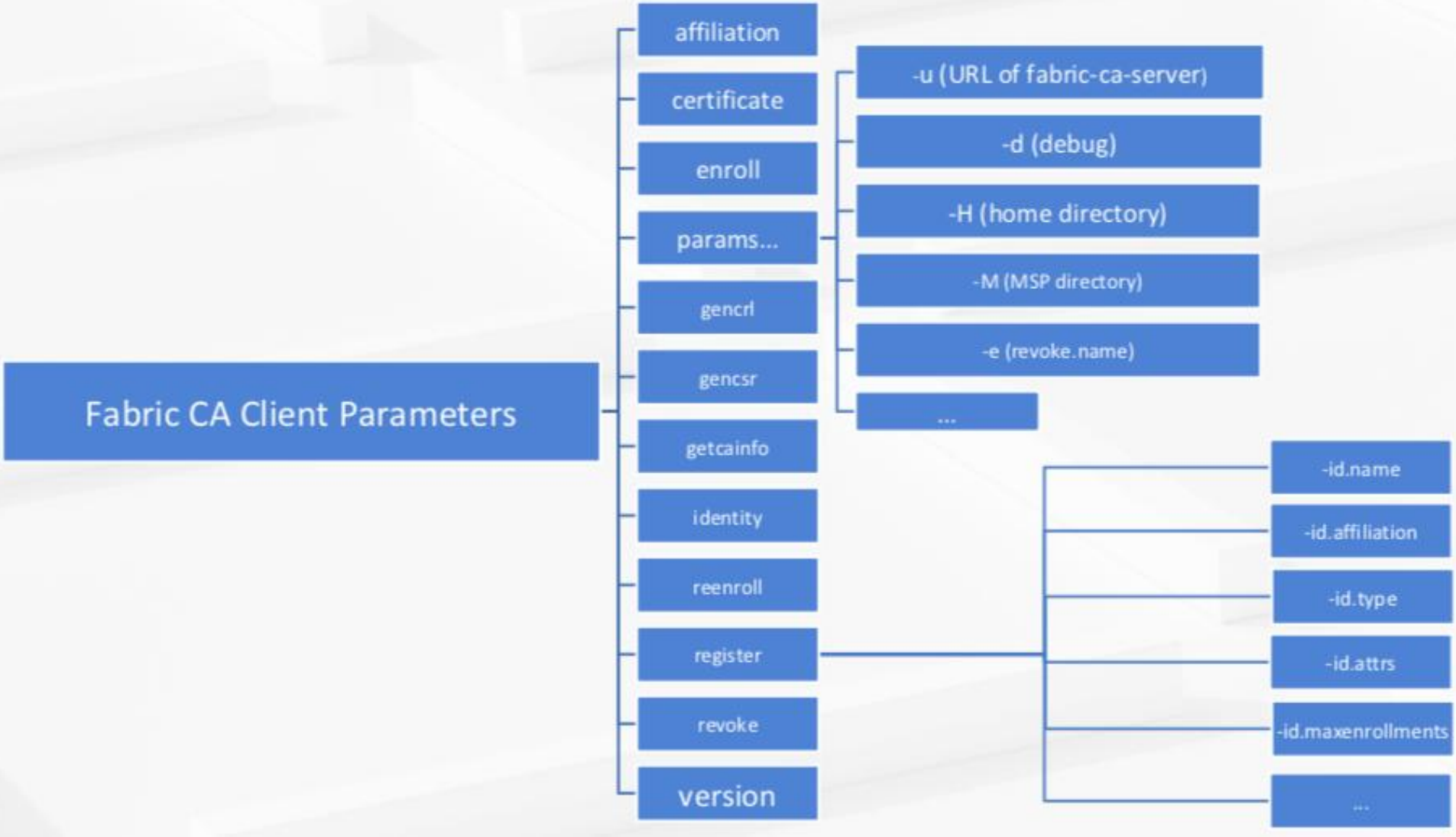


Intermedia CA

- 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



Fabric CA Client



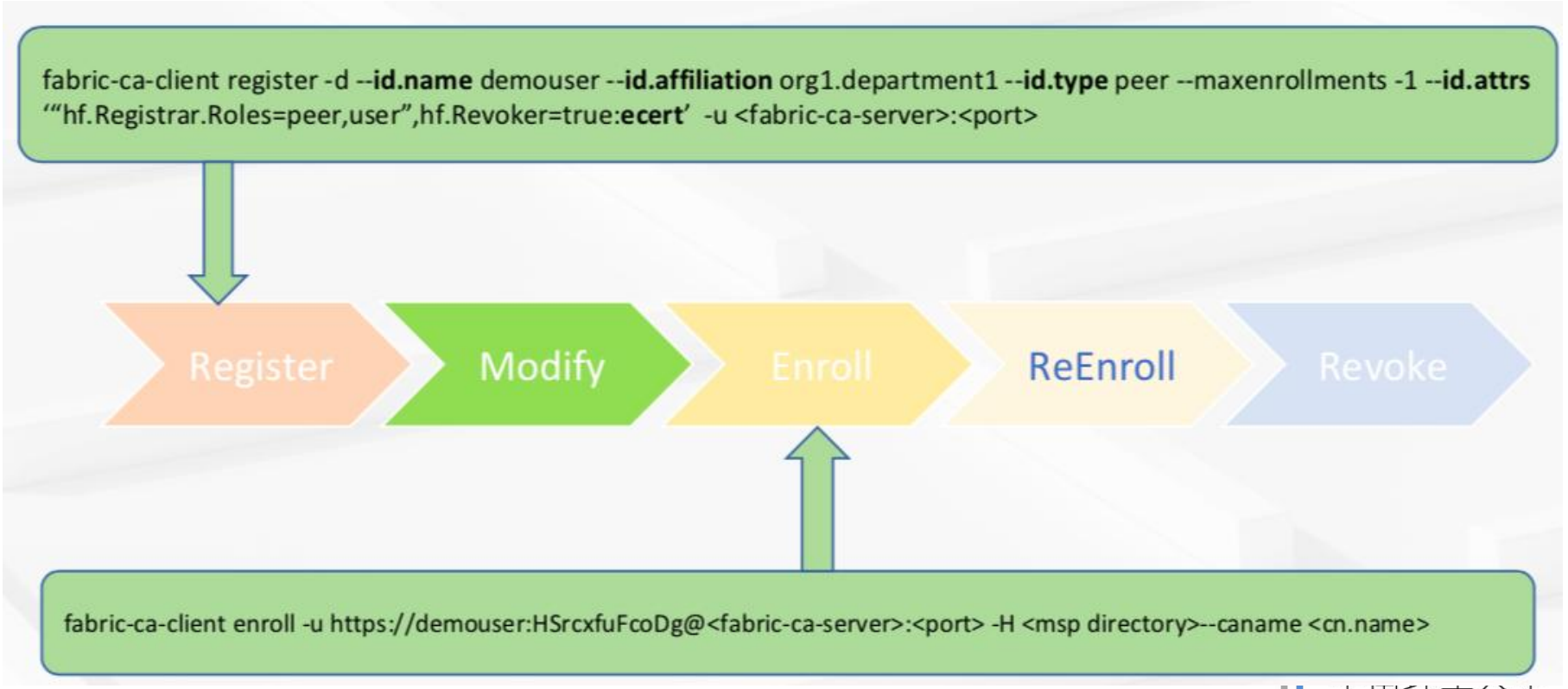
ABAC(Attribute-Based Access Control)

- 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

注册（register）：根据提供的用户名、用户类型和组织关系等属性注册一个用户账号，此时只会将新用户的信息保存到ca-server中，而不会在本地生成对应的msp
登记（enroll）：即载入，根据register过的用户信息生成其msp，并将msp加载到本地

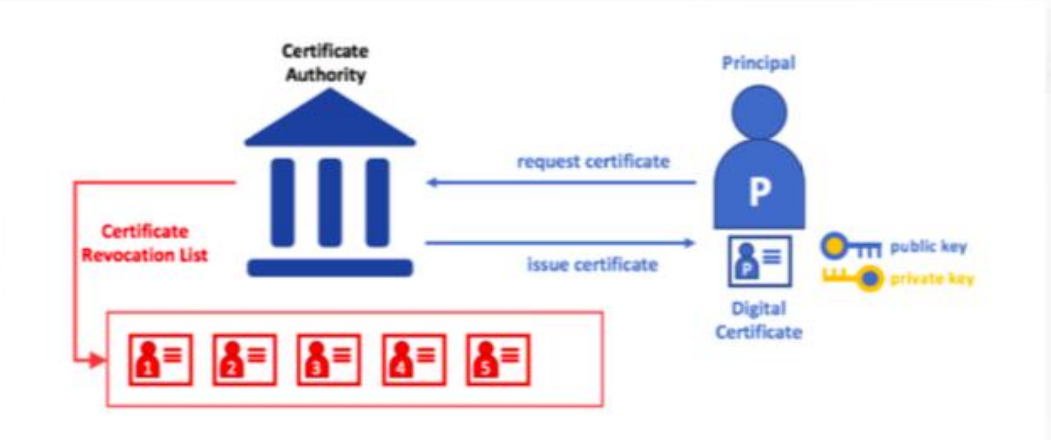


Part 2

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

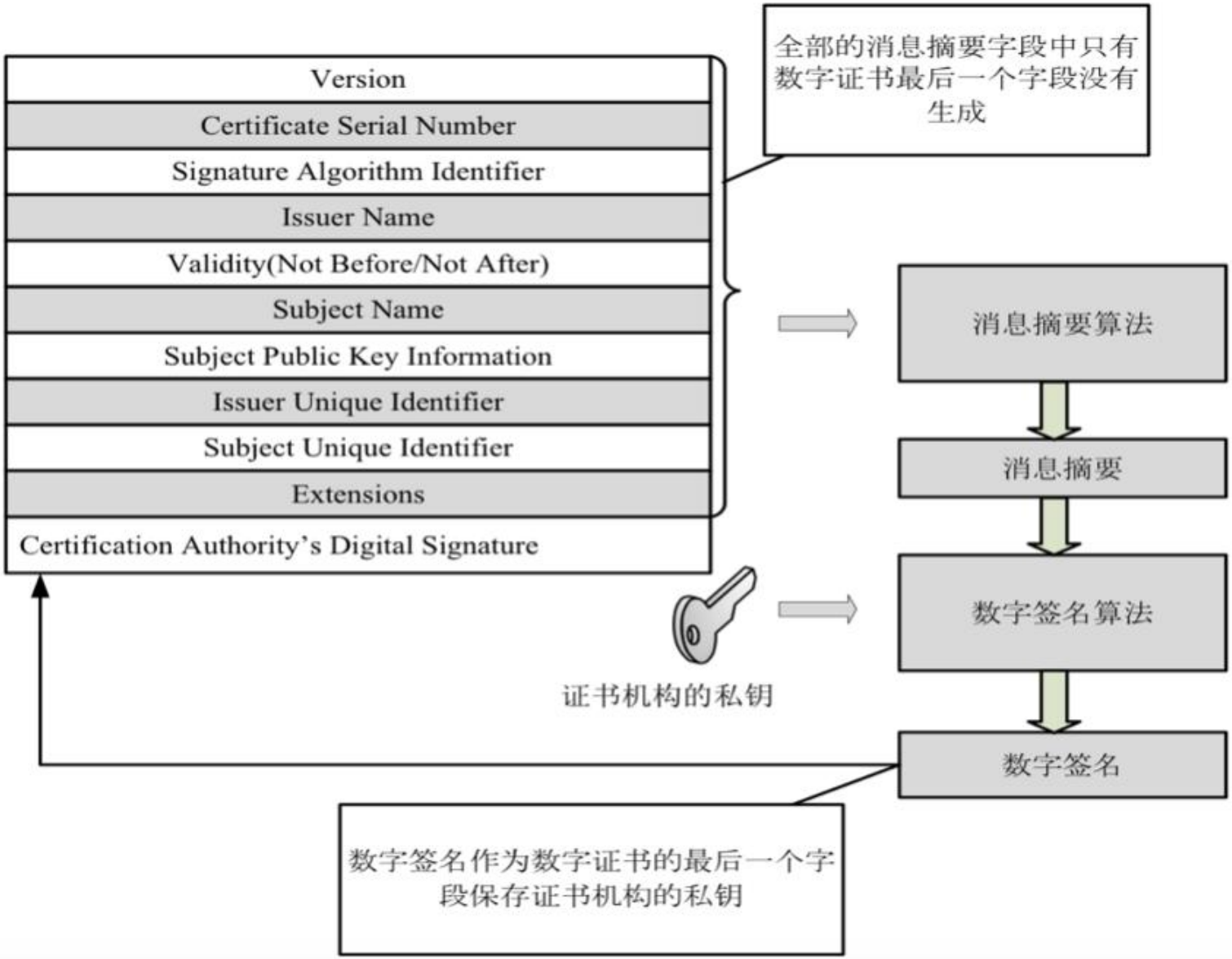
X.509 cert content：

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

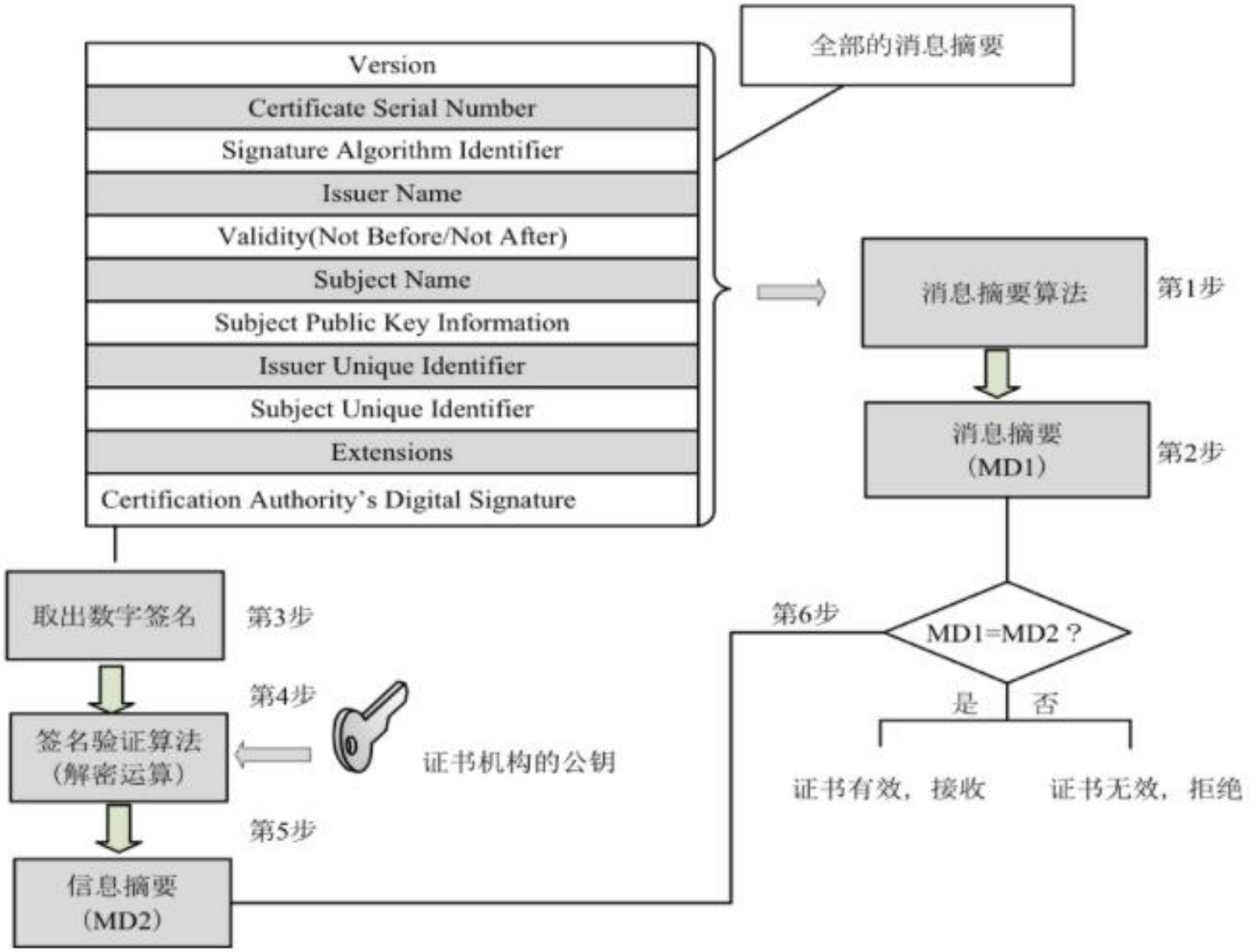
Three types of certifications

- ECert：颁发给提供了注册凭证的用户或节点实体，长期有效。（主要就是通ECert对实体身份检验）
- TLSCert：TLS证书用来保障通信链路安全，控制对网络层的接入访问，可以对远端实体身份校验，防止窃听。
- TCert：颁发给用户，控制每个交易的权限，一般针对某个交易，短期有效。

Sign certifications



Verify the certifications



理工大学

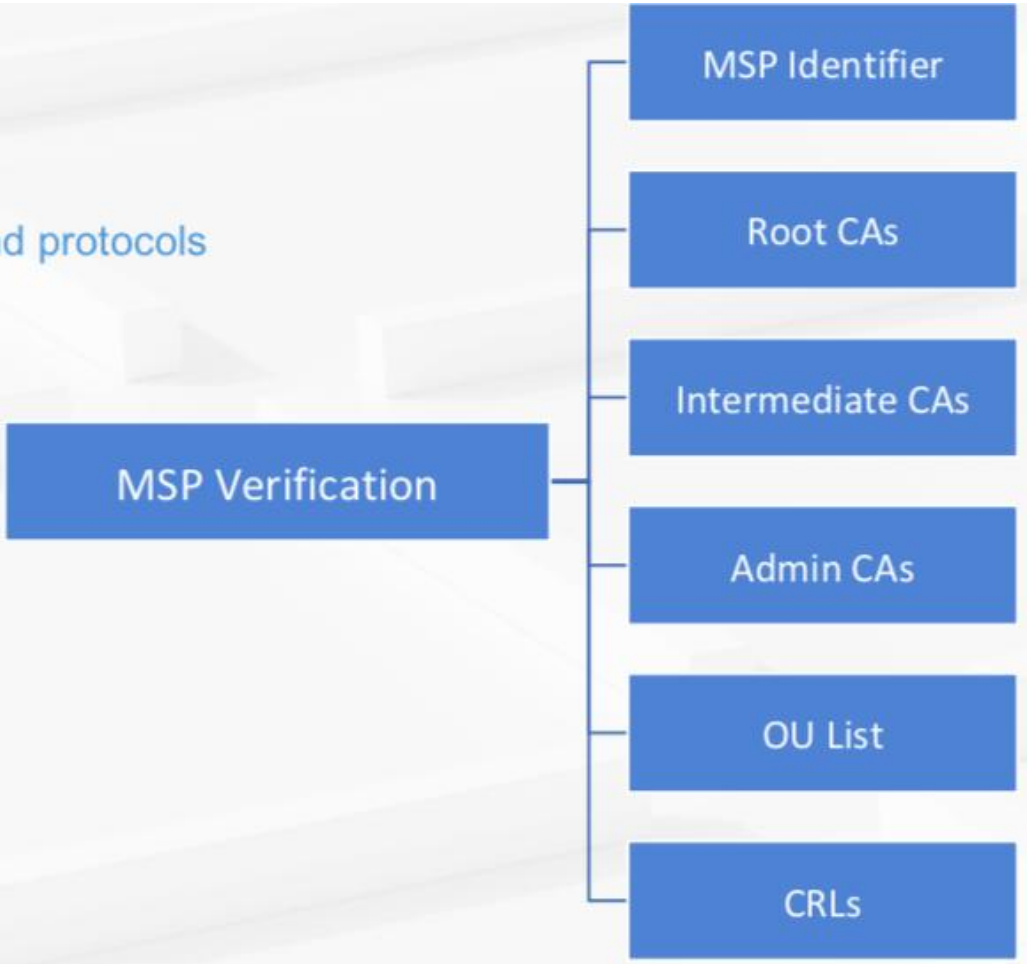
Part 3

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 …

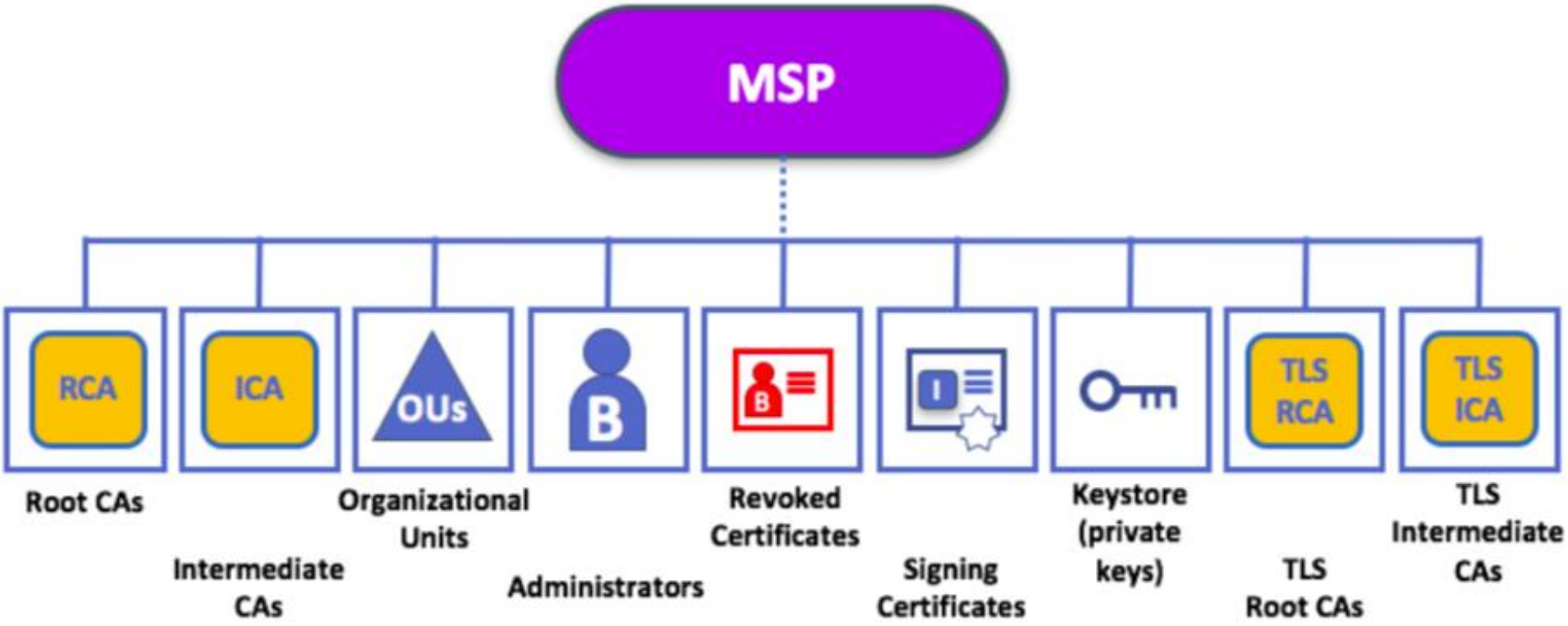


BCCSP

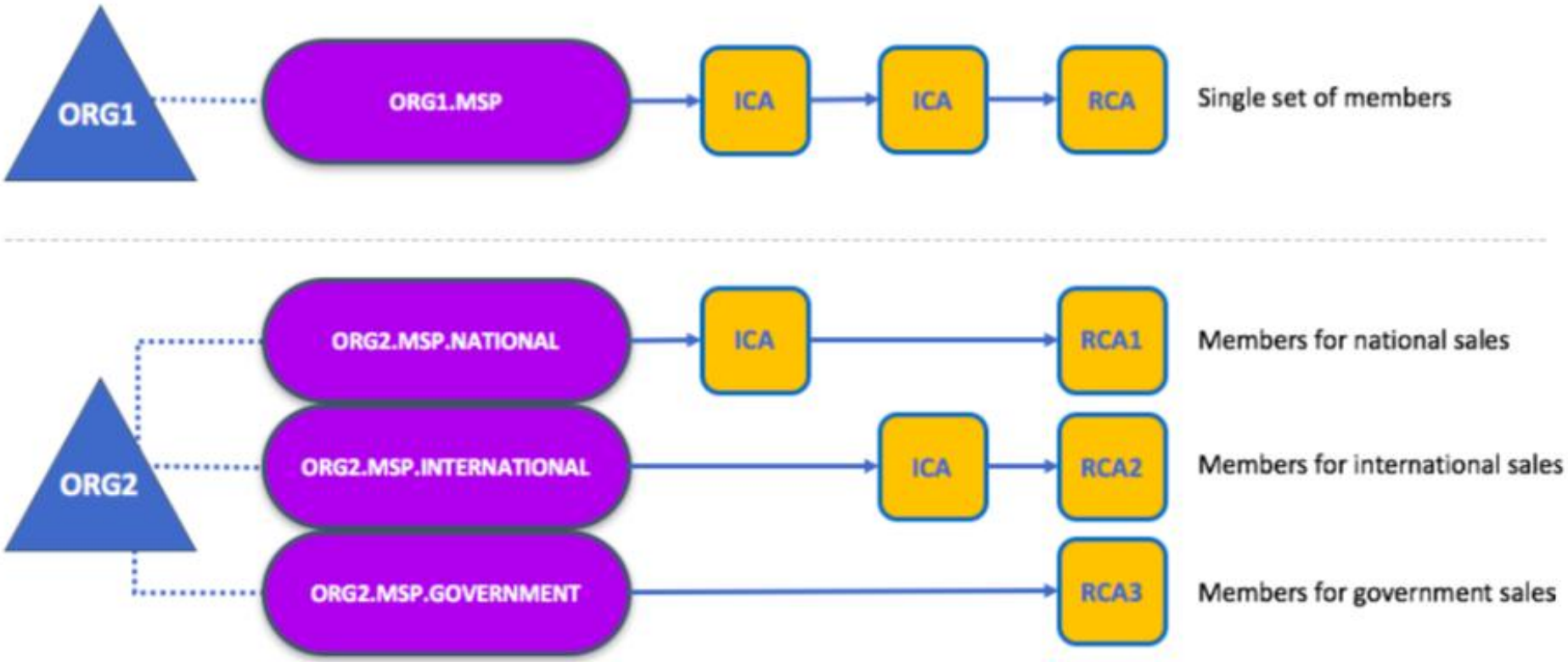
- Blockchain cryptographic service provider
- Implementation:
  - PKCS #11
  - SW

```
###############################################################################
# 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
```

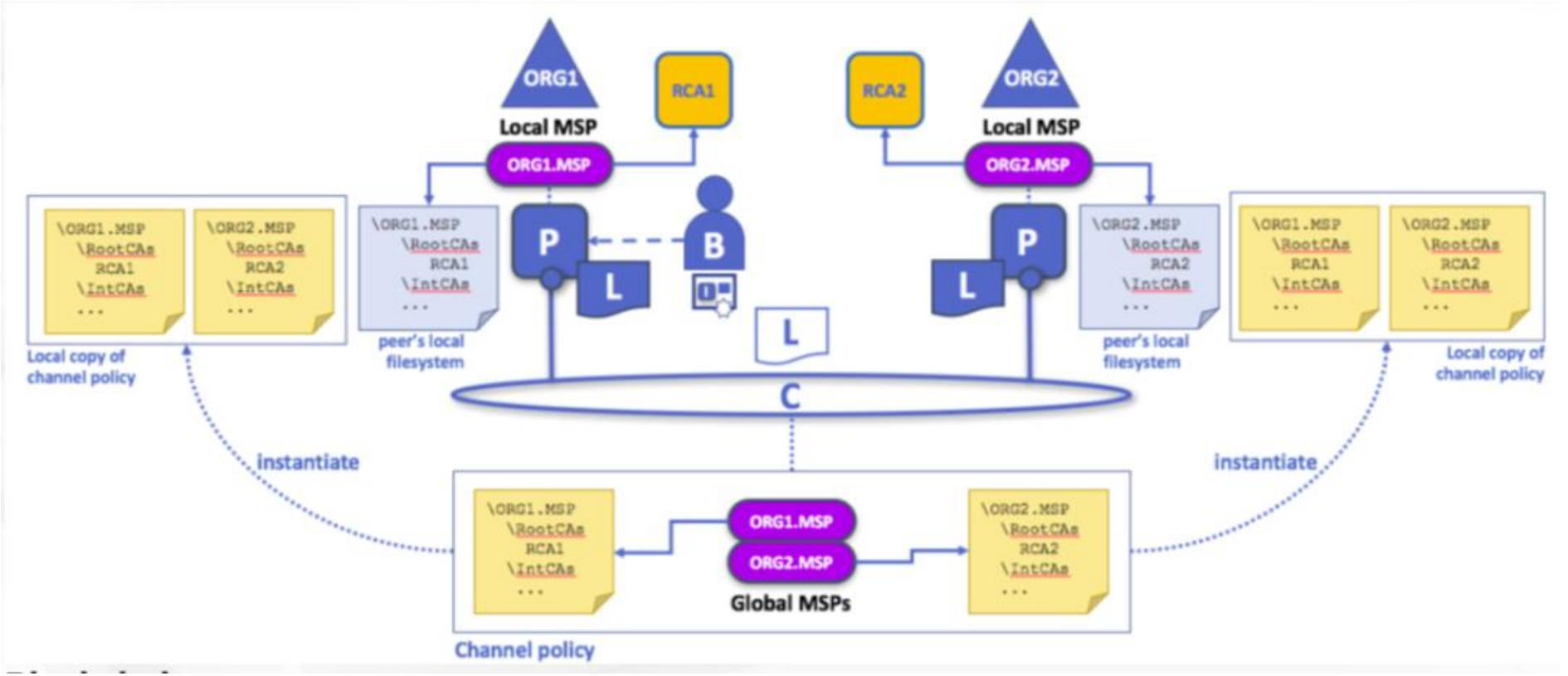
MSP Tree


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

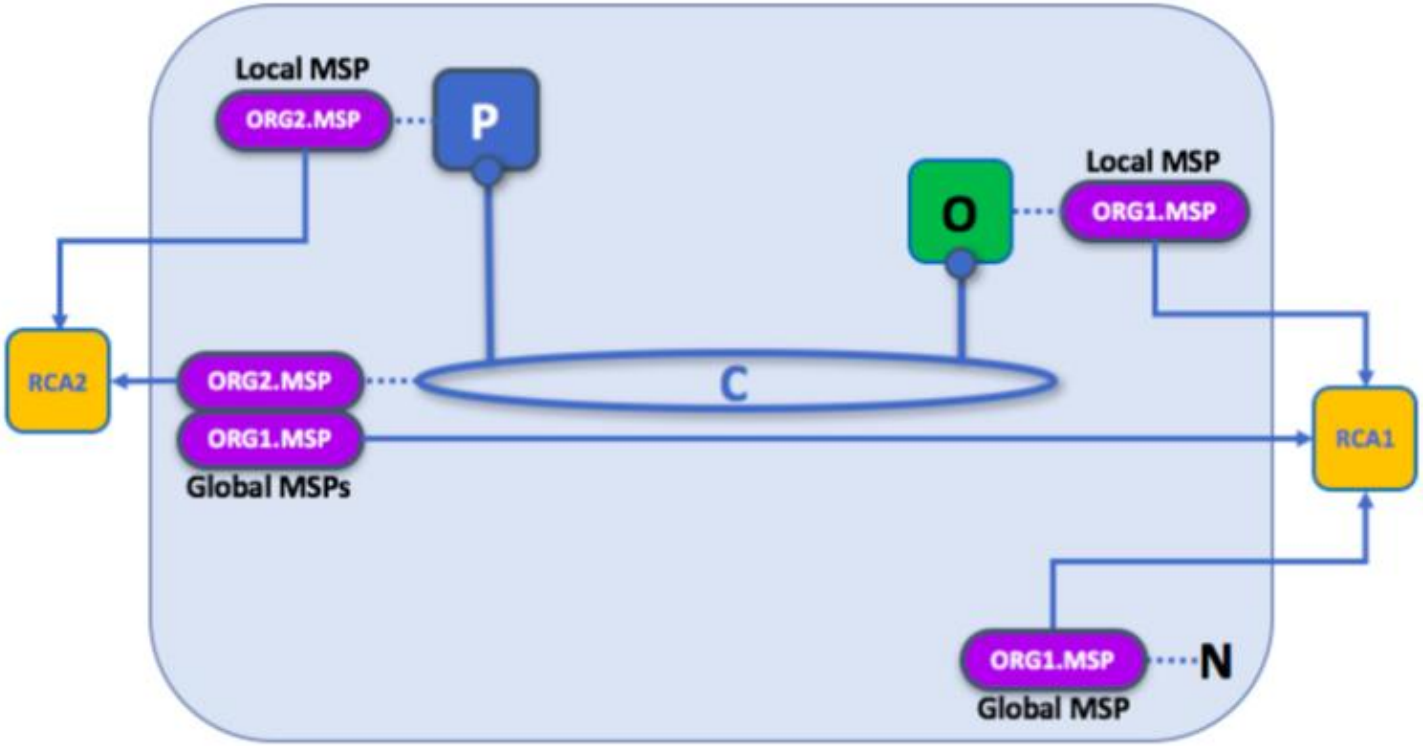
Organization - MSP



MSP in Channel



MSP Level



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

Thanks!