Fabric 用户管理及权限验证

董振华
dongzh@cn.ibm.com
IBM区块链平台产品经理

Identity

- Fabric网络的各种参与者，包括peers, orderers, client applications, administrators，由X.509数字证书表示其身份Identity

- 参与者在Fabric网络中的权限由identity中的properties（组织，角色，属性等）决定，properties记录在X.509数字证书中。

Fabric 1.1 新功能 – 基于属性的访问控制

- Fabric-ca register 或 enroll 一个用户时，可为其添加属性，反应在x509证书的X509v3 extensions中

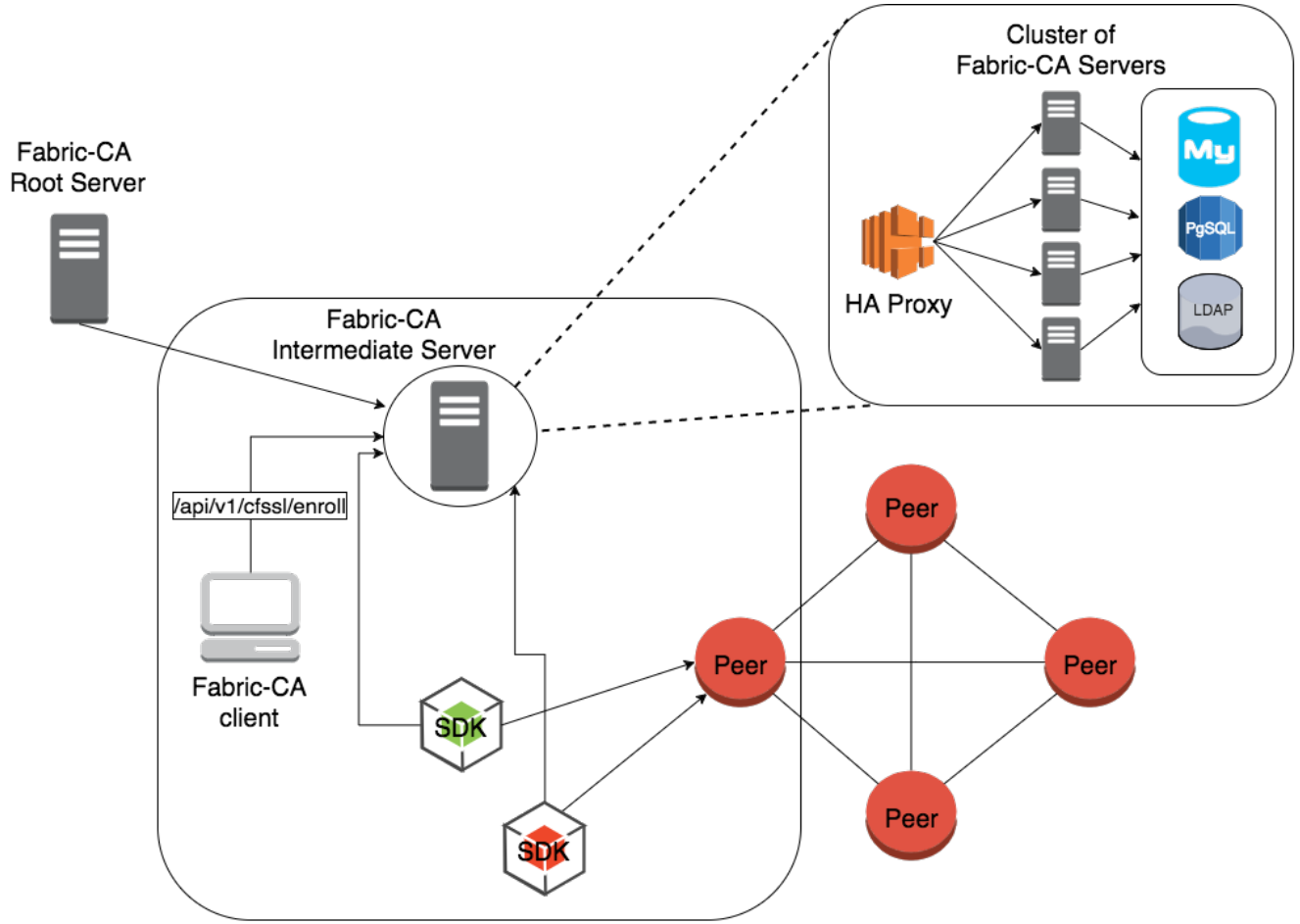
- Chaincode中，可根据用户所属的MSPID和持有的属性值进行区分

```
Certificate:
    Data:
     .....
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign
         .....
            X509v3 Subject Alternative Name:
                DNS:Anils-MacBook-Pro.local
            1.2.3.4.5.6.7.8.1:
                {"attrs":{”trader":”true"}}
    Signature Algorithm: ecdsa-with-SHA256
    .....
```

```
import "github.com/hyperledger/fabric/core/chaincode/lib/cid"
// Get the client ID object
id, err := cid.New(stub)
if err != nil {
  // Handle error
}
mspid, err := id.GetMSPID()
if err != nil {
  // Handle error
}
switch mspid {
  case "org1MSP":
    err = id.AssertAttributeValue(”trader", "true")
  case "org2MSP":
    err = id.AssertAttributeValue(“sales", "true")
  default:
    err = errors.New("Wrong MSP")
}
```

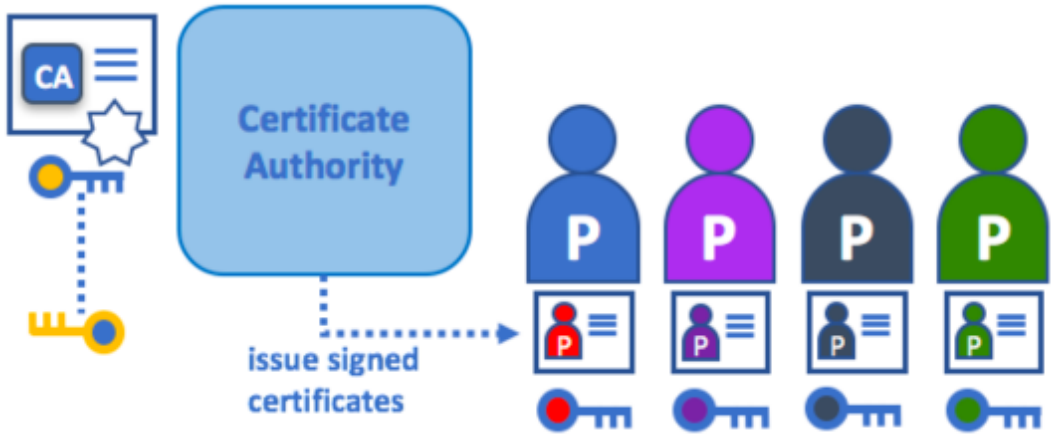
CA 部署

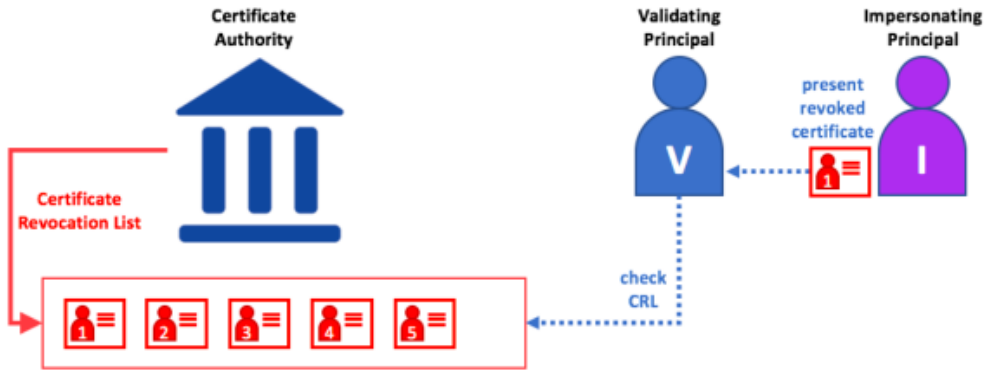
- Fabric-CA作为root CA和intermediate CA
- Fabric-CA作为intermediate CA (intermediate signing certificate由外部CA生成)
- 全部使用外部CA
  - 考虑 Rest API, attribute, etc.



Fabric-CA

- 区块链网络的各个参与方有自己相应的CA，代表参与方进行操作的终端用户需要进行以下操作才能获得相应权限：
  - 在Fabric-CA中注册（register）一个用户，需要有register权限的Fabric-CA用户来为其他用户进行注册；
  - 用已注册的用户名 / 密码通过enroll操作获得CA证书，用户私钥及证书保存在应用端本地。
- 用户持有自己的证书进行交易并用私钥进行签名，区块链网络中的节点及channel已经有各个Fabric-CA的根证书信息，可以验证用户的身份及签名；
- 用户证书过期前可通过reenroll进行更新，有权限的用户可以revoke其他用户的证书。
- 具有hf.GenCRL属性的用户可生成CRL（Certificate Revocation List）置于节点MSP目录中，以便无效证书的核实





Fabric-CA Restful Services

- “/api/v1/cainfo” : Get CA information
- “/api/v1/enroll” : Enroll a new identity and return an enrollment certificate (provide enrollment ID and secret)
- “/api/v1/reenroll” : Reenroll an enrollment certificate
- “/api/v1/register” : Register a new identity with the Fabric CA server
- “/api/v1/revoke” : Revoke a specific certificate identified by a SN and AKI or all certificates associated with the identity.
- “/api/v1/gencrl” : Generates a Certifcate Revocation List
- “/api/v1/affiliations” : The caller must have **hf.AffiliationMgr** authority
  - get : List all affiliations equal to and below the caller's affiliation
  - post: Create a new affiliation
- "/api/v1/affiliations/{affiliation}” : The caller must have **hf.AffiliationMgr** authority
  - get : List a specific affiliation at or below the caller's affinity
  - put : Rename an affiliation.
  - delete : Delete a specific affiliation
- "/api/v1/identities” : The caller must have **hf.Registrar** authority
  - get : List all identities that the caller is entitled to see
  - post : Create a new identity with the Fabric CA server.
- "/api/v1/identities/{id}” : The caller must have **hf.Registrar** authority
  - get : Get an identity
  - put : Update an existing identity (type, secret, etc.)
  - delete: Delete an existing identity

MSP与创始块

- 区块链网络管理员可在配置文件config.yaml 中指定每个组织的MSP ID和其对应文件组的路径，Fabric的configtx工具根据config.yaml中的配置生成
  - 区块链网络的创世区块：Orderer启动时需提供的 .block文件
  - 某一通道的配置：创建通道时需提供的 .tx文件。

- 创世区块中带有了证书，CRL等信息。orderer和加入某一通道的peer对这些信息进行解析保存，进而可以通过用户的签名去验证其操作是否合法。

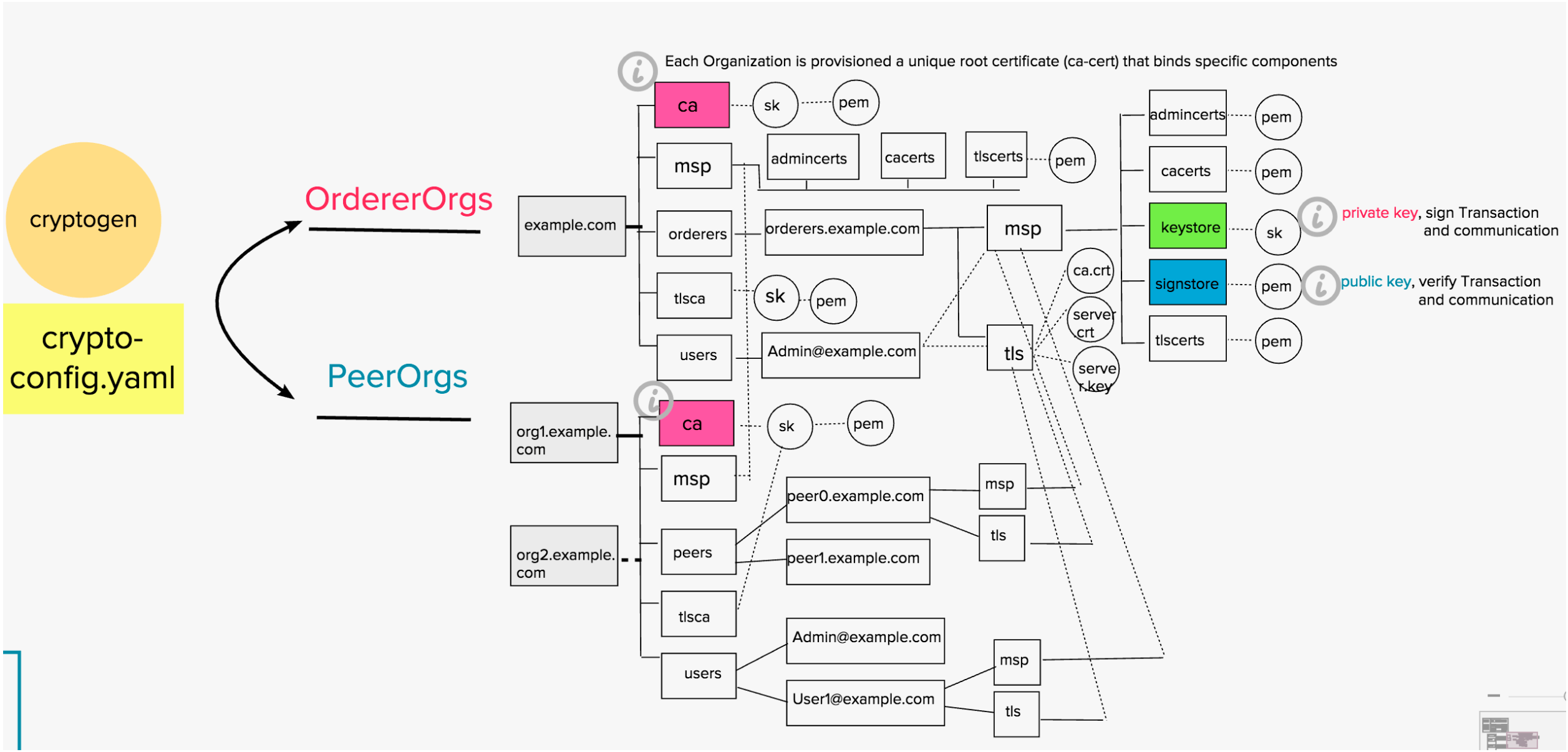
```
Organizations:

    # SampleOrg defines an MSP using the sampleconfig.  It should never be used
    # in production but may be used as a template for other definitions
    - &OrdererOrg
        # DefaultOrg defines the organization which is used in the sampleconfig
        # of the fabric.git development environment
        Name: OrdererMSP

        # ID to load the MSP definition as
        ID: OrdererMSP

        # MSPDir is the filesystem path which contains the MSP configuration
        MSPDir: crypto-config/ordererOrganizations/example.com/msp

    - &Org1
        # DefaultOrg defines the organization which is used in the sampleconfig
        # of the fabric.git development environment
        Name: Org1MSP

        # ID to load the MSP definition as
        ID: Org1MSP

        MSPDir: crypto-config/peerOrganizations/org1.example.com/msp

        AnchorPeers:
            # AnchorPeers defines the location of peers which can be used
            # for cross org gossip communication.  Note, this value is only
            # encoded in the genesis block in the Application section context
            - Host: peer0.org1.example.com
              Port: 7051
```

Local MSP

- peer和orderer节点在启动时需要根据参数初始化MSP。目前MSP支持两种类型，bccsp（默认）和idemix（更强的隐私保护），开发者可根据需求实现其他类型的MSP。
- 初始化方法获取MSP配置信息，以bccsp msp为例，将mspConfigPath目录中的CA证书，Admin证书，TLSCA证书，CRL等信息进行处理填充进MSP实例。
- 当peer和orderer节点启动后，MSP负责证书校验，签名核实和身份认证。vscc（Validate System Chaincode）负责背书的校验，就是验证（每个）签名的有效性，以及是否符合背书策略（有效签名个数是否满足）。

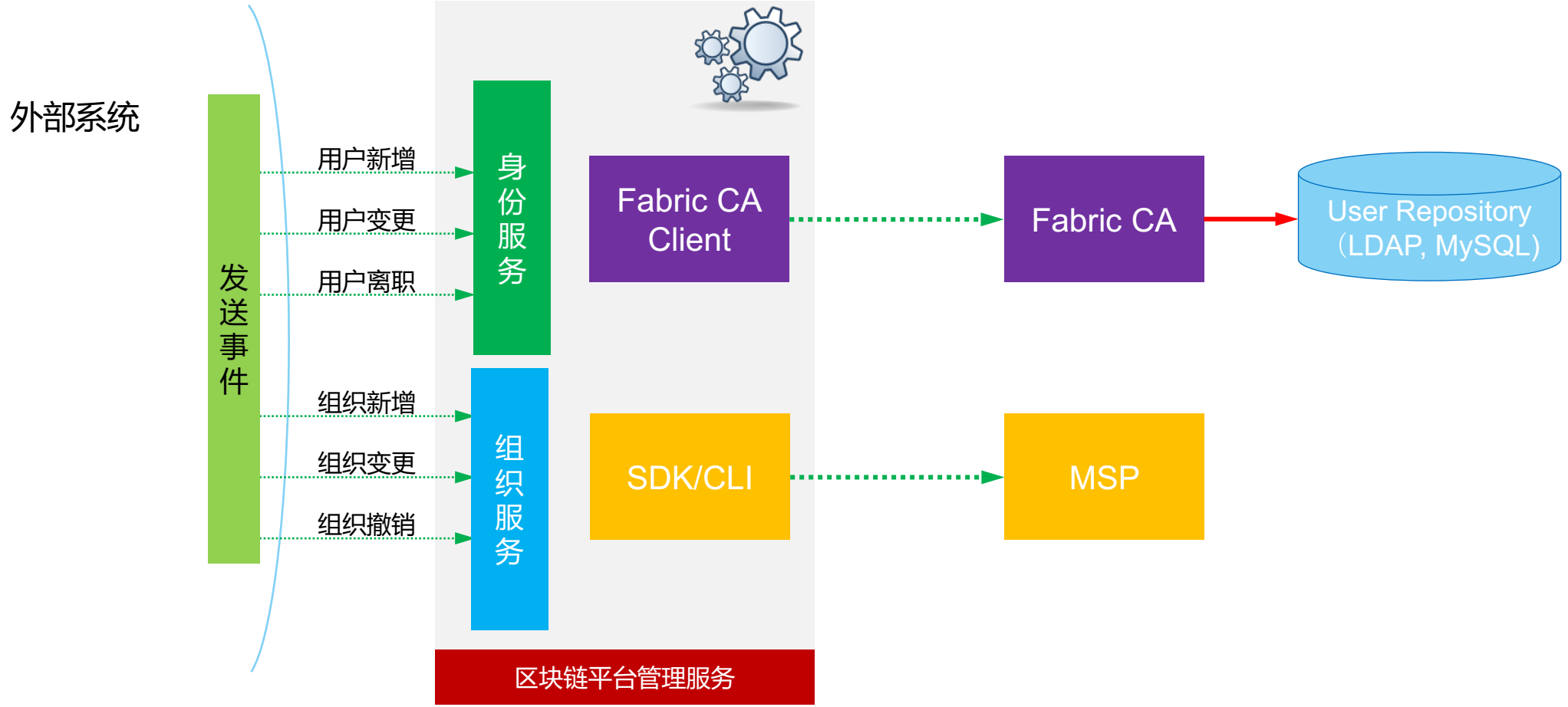
```
orderer.example.com:
    container_name: orderer.example.com
    environment:
      - ORDERER_GENERAL_GENESISMETHOD=file
      - ORDERER_GENERAL_GENESISFILE=/etc/hyperledger/configtx/twoorgs.genesis.block
      - ORDERER_GENERAL_LOCALMSPID=OrdererMSP
      - ORDERER_GENERAL_LOCALMSPDIR=/etc/hyperledger/msp/orderer
      - ORDERER_GENERAL_LOCALMSPTYPE=BCCSP
  ......
  peer0.org1.example.com:
    container_name: peer0.org1.example.com
    environment:
      - CORE_PEER_ID=peer0.org1.example.com
      - CORE_LOGGING_LEVEL=debug
      - CORE_PEER_LOCALMSPID=Org1MSP
      - CORE_PEER_MSPCONFIGPATH=/etc/hyperledger/msp/peer/
      - CORE_PEER_LOCALMSPTYPE=BCCSP
  ......
```

MSP文件结构


cryptogen
crypto-config.yaml
OrdererOrgs
PeerOrgs
Each Organization is provisioned a unique root certificate (ca-cert) that binds specific components
example.com
ca
sk
pem
msp
admincerts
cacerts
tlscerts
pem
orderers
orderers.example.com
msp
admincerts
pem
cacerts
pem
keystore
sk
private key, sign Transaction and communication
signstore
pem
public key, verify Transaction and communication
tlscerts
pem
tlsca
sk
pem
users
Admin@example.com
ca.crt
server crt
server.key
tls
org1.example.com
ca
sk
pem
msp
peer0.example.com
msp
tls
org2.example.com
peers
peer1.example.com
tlsca
Admin@example.com
users
msp
User1@example.com
tls

Fabric用户与外部用户 同步 or 独立

- 身份服务
  - –外部系统通过固定的Fabric用户，进行区块链操作
  - –外部系统作为 “上游”身份源，驱动区块链“身份服务”创建 / 变更相关的用户
- 组织服务：更新Channel的config block进行组织信息的修改



Thanks