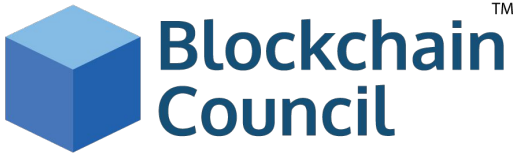


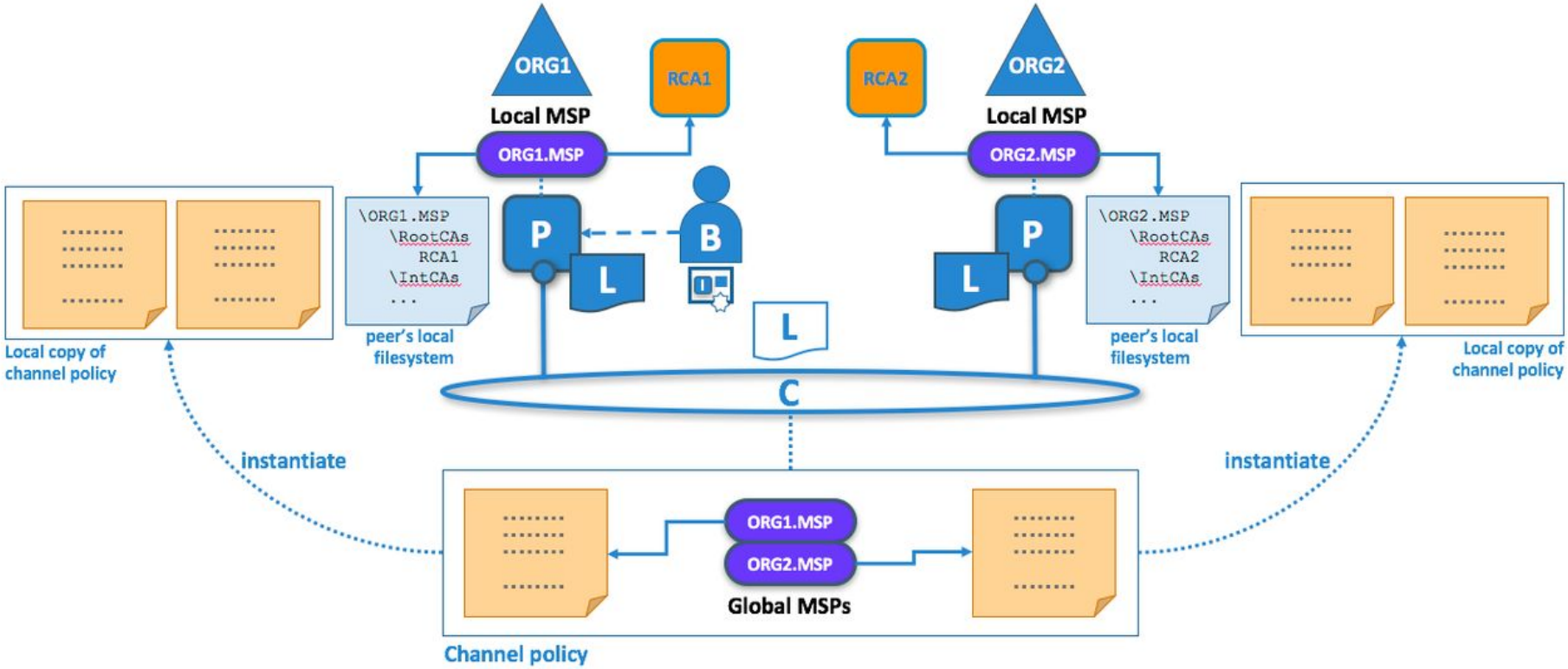
Certified Hyperledger Expert

Hyperledger Fabric Membership Service Provider

Introduction

- MSP is a Membership Service Provider pluggable interface to support variety of credentials architectures.
- A Membership Service Provider involves these key aspects for its proper functioning:
  - Concrete identity format
  - User credential validation
  - User credential revocation
  - Signature generation and verification
- A Hyperledger Fabric blockchain network can be governed by one or more MSPs, which provides modularity of membership operations, and interoperability across different membership standards.

Membership Service Provider



How to use MSP?

- The MSP must be installed on each channel peer to ensure that transaction requests that are issued to the peer originate from an authenticated and authorized user identity.
- A MSP Identifier or MSP ID needs to be specified for each MSP, in order to reference that MSP in the network which must be unique per MSP instance.
- If default implementation of MSP is chosen, a set of parameters are required to be specified to allow for identity validation and signature verification, this includes:
    - A list of self-signed (X.509) certificates to represent intermediate CAs
    - A list of X.509 certificates to represent the administrators of this MSP
    - A list of valid members of this MSP
    - A list of certificate revocation lists (CRLs)
    - A list of X.509 certificates to represent intermediate TLS CAs
    - A list of self-signed (X.509) certificates of TLS root of trust for TLS certificate

MSP’s valid identity rule

- Valid and authorized identities for the MSP instance are required to satisfy the following list conditions:
  - MSP instance should be in the form of X.509 certificates with a verifiable certificate path to exactly one of the root of trust certificates.
  - MSP instance should not be included in any CRL.
  - MSP instance lists one or more of the Organizational Units of the MSP configuration in the OU field of their X.509 certificate structure.

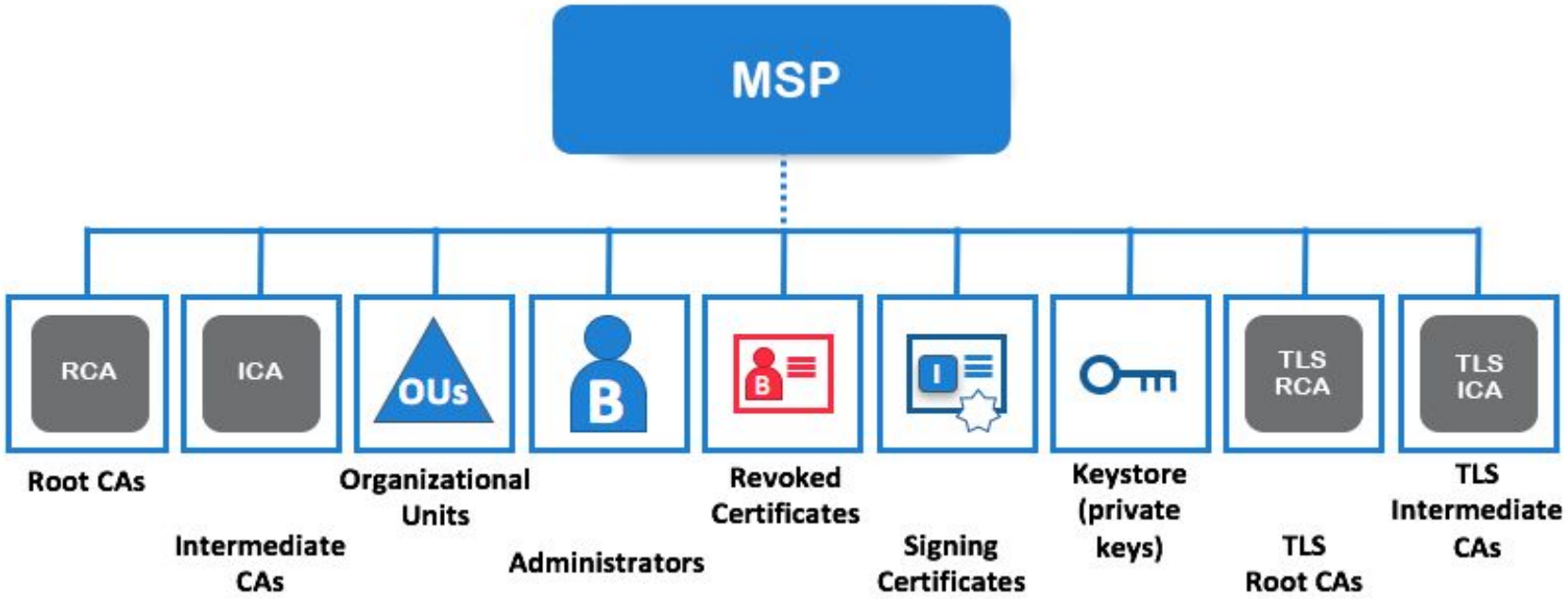
Generating MSP certificates

- For generating X.509 certificates to feed its MSP configuration, application can use:
  - Openssl.
  - Cryptogen tool
  - Hyperledger Fabric CA

MSP setup

- To set up a local MSP (for either a peer or an orderer), the administrator should create a folder that contains these subfolders and a file:
  - admincerts
  - intermediatecerts
  - keystore
  - tlscacerts
  - config.yaml file
  - cacerts
  - crls
  - signcerts
  - tlsintermediatecerts
- In the configuration file of the node (core.yaml file for the peer, and orderer.yaml for the orderer), one needs to specify the path to this folder, and the MSP Identifier of the node's MSP.

MSP components



THANK YOU!

Any questions?

You can mail us at

hello@blockchain-council.org