Membership and Identity Management

Organization

- Legal entities, Define boundaries within a Fabric.
- Each organization defines :-
  - MSP for identities
  - Administrator(s)
  - Users
  - Peers
  - Orderers (optional)
  - A network may include many organization to form a consortium.
  - Each organization has an ID.

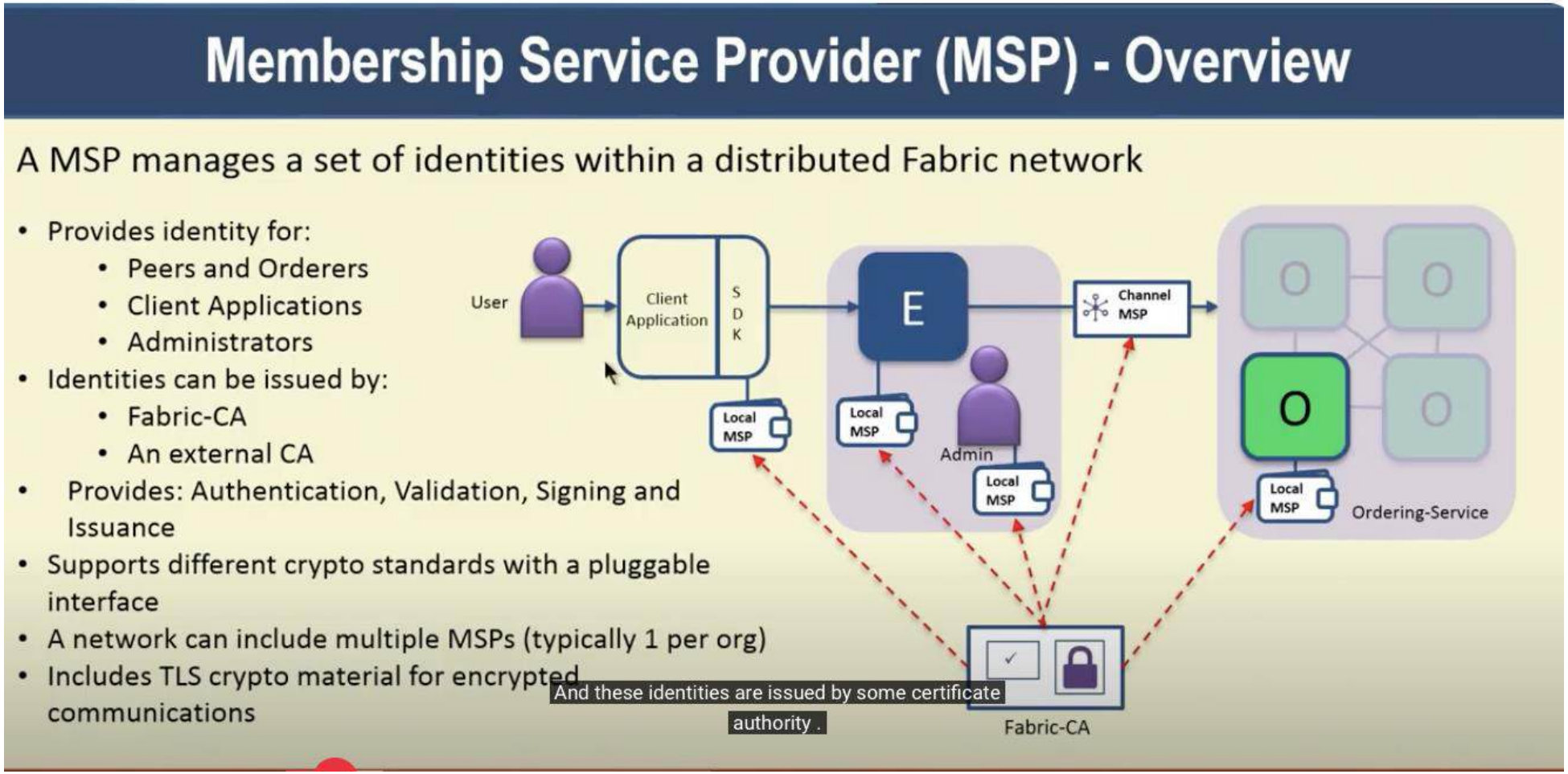
MSP -why do we need MSP ?

- Certificate Authorities issue identities by generating a public and private key which forms a key-pair that can be used to prove identity. This identity needs a way to be recognized by the network, which is where the MSP comes in.
- For example, a peer uses its private key to digitally sign, or endorse, a transaction. The MSP is used to check that the peer is allowed to endorse the transaction. The public key from the peer’s certificate is then used to verify that the signature attached to the transaction is valid. Thus, the MSP is the mechanism that allows that identity to be trusted and recognized by the rest of the network.

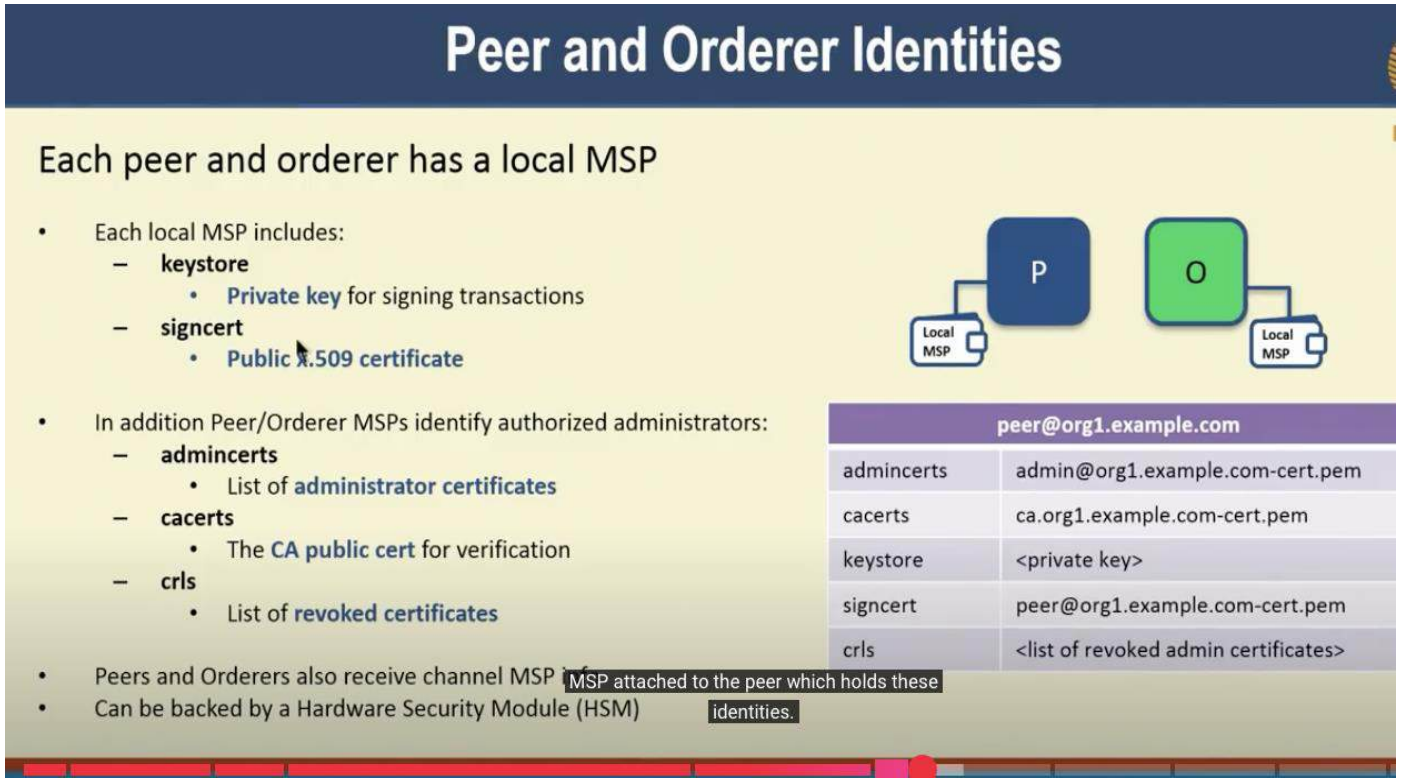
MSP-Overview

- Manages a set of identities within a distributed Fabric N/w.
- Provides identities for
  - Peers and Orderers
  - Client Application
  - Administrators
- Identities can be issued by
  - Fabric CA
  - External CA

MSP-Oveview


Membership Service Provider (MSP) - Overview
A MSP manages a set of identities within a distributed Fabric network
• Provides identity for:
• Peers and Orderers
• Client Applications
• Administrators
• Identities can be issued by:
• Fabric-CA
• An external CA
• Provides: Authentication, Validation, Signing and Issuance
• Supports different crypto standards with a pluggable interface
• A network can include multiple MSPs (typically 1 per org)
• Includes TLS crypto material for encrypted communications
User
Client Application
S D K
Local MSP
E
Local MSP
Admin
Local MSP
Channel MSP
O
Local MSP
Ordering-Service
And these identities are issued by some certificate authority .
Fabric-CA

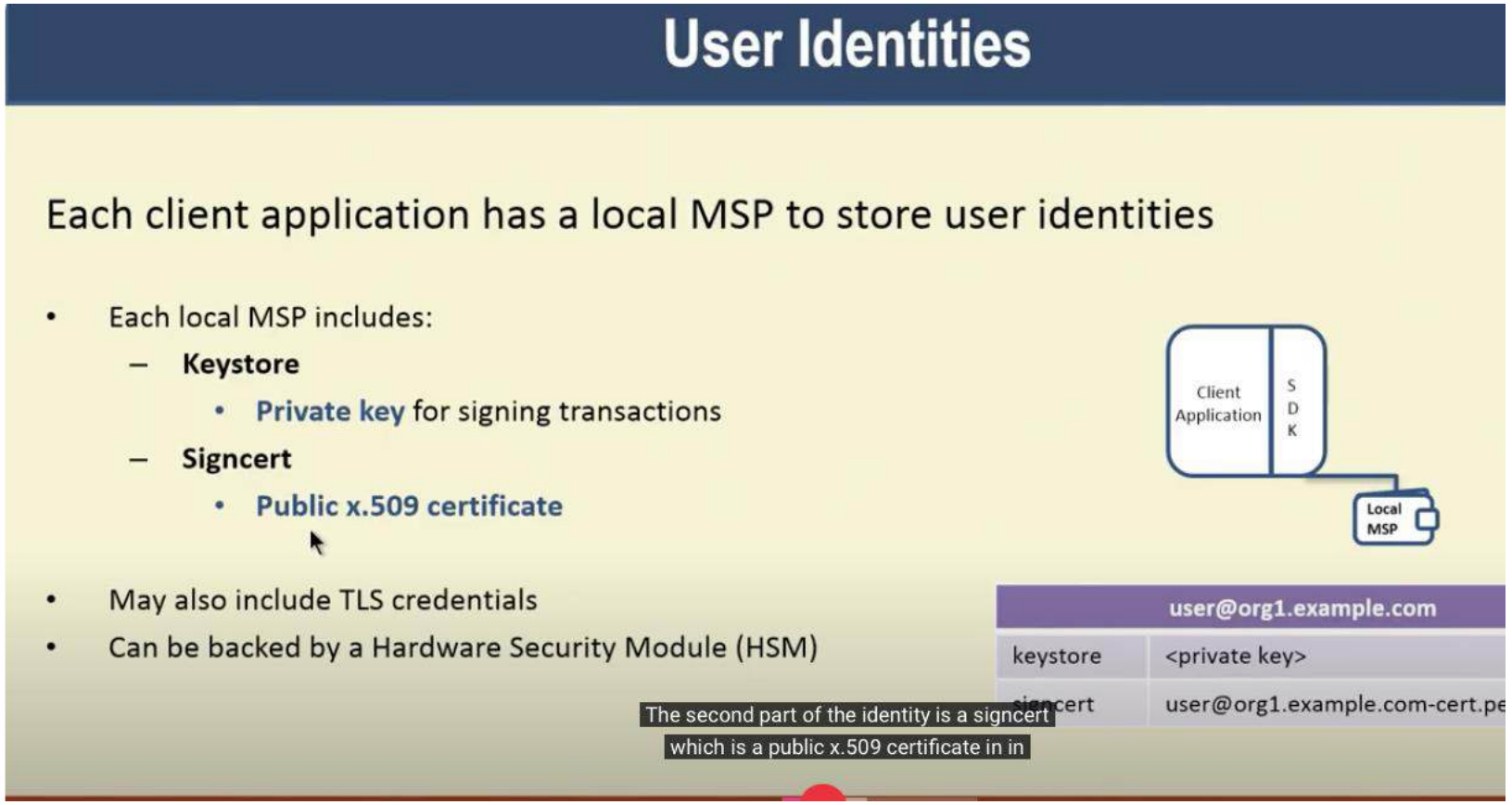
Peer and Orderer Identites



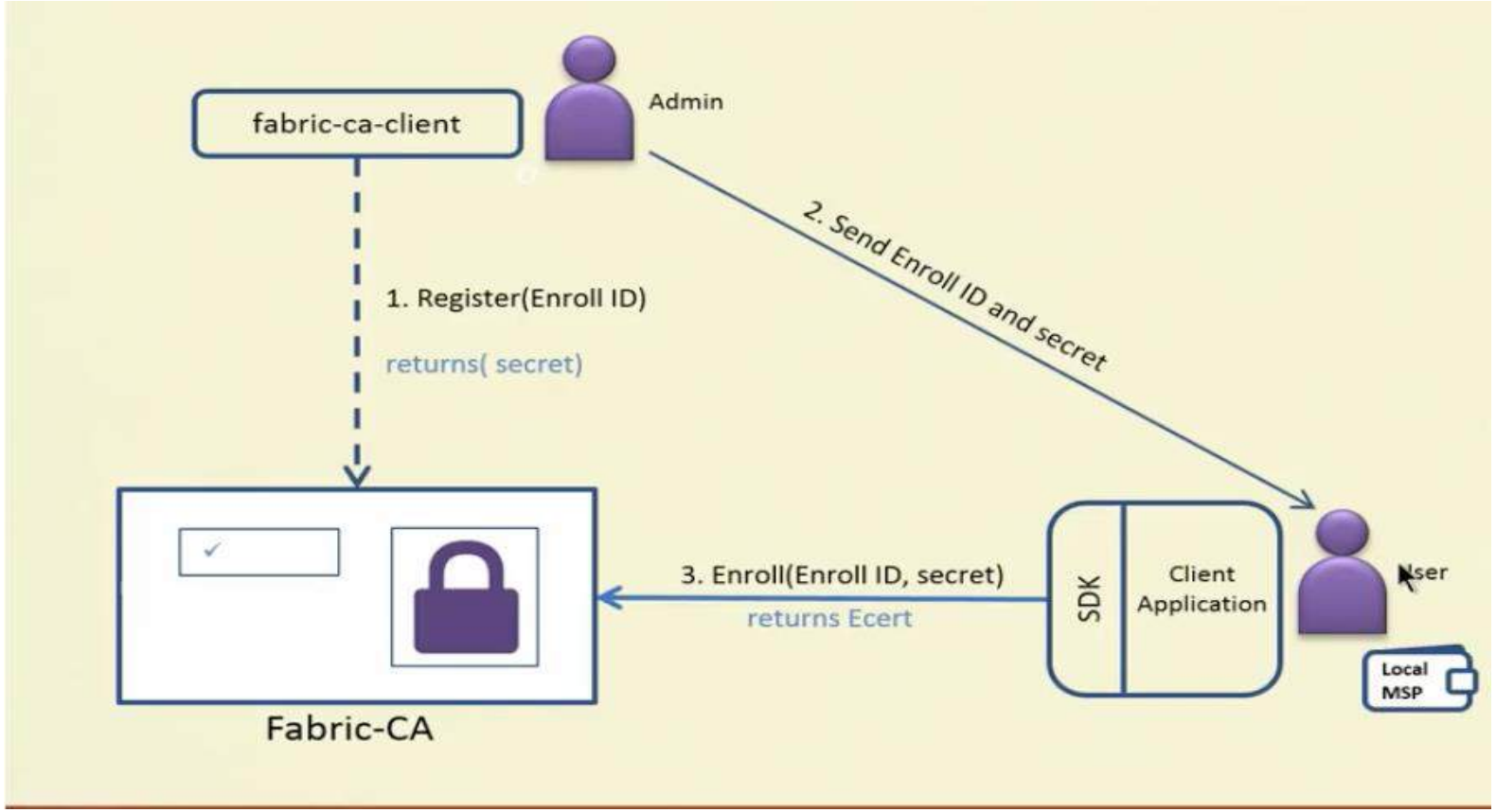
Channel MSP


Channel MSP Information
Channels include additional organisational MSP information
Determines which orderers or peers can join the channel
Determines client applications read or write access to the channel
Stored in configuration blocks in the ledger
Each channel MSP includes:
admincerts
Any public certificates for administrators
cacerts
The CA public certificate for this MSP
crls
List of revoked certificates
Does not include any private keys for identity
admincerts
cacerts
crls
channel and this can be dynamic

User Identities



New User Registration and Enrollment



Transaction Signing