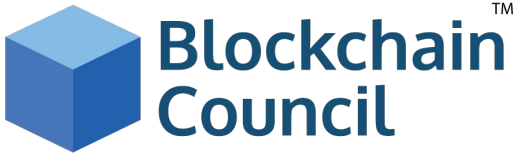

Certified Hyperledger Developer

Access Control Logic

Access control rules

- In this file we defined the rules or permissions for different users based on their identity.
- Here we have defined multiple rules for both partner access and member access.
- We have also defined the rules for: access control for resources within a business network (business access control) and access control for network administrative changes (network access control).

Network access control

- We have grant business network administrators full access to user resources

```
rule NetworkAdminUser {
      description: "Grant business network administrators full access to user
      resources"
      participant: "org.hyperledger.composer.system.NetworkAdmin"
      operation: ALL
      resource: "**"
      action: ALLOW
}
```

Network access control

- We have grant business network administrators full access to system resources

```
rule NetworkAdminSystem {
      description: "Grant business network administrators full access to system
      resources"
      participant: "org.hyperledger.composer.system.NetworkAdmin"
      operation: ALL
      resource: "org.hyperledger.composer.system.**"
      action: ALLOW
}
```

Member access rules

- Members to have access only to their own account

```
rule MemberAccessOwnRecord {
      description: "Allow Member to access only their profile"
      participant(p): "org.clp.biznet.Member"
      operation: ALL
      resource(r): "org.clp.biznet.Member"
      condition: (r.getIdentifier() === p.getIdentifier())
      action: ALLOW
}
```

Member access rules

- Members Not to have access to other member accounts

```
rule MemberAccessMembers {
   description: "Deny Member access to other Member accounts"
   participant: "org.clp.biznet.Member"
   operation: ALL
   resource: "org.clp.biznet.Member"
   action: DENY
}
```

Member access rules

- Members have access to Partners on the network

```
rule MemberAccessPartners {
    description: "Allow Member access to all Partners on the network"
    participant: "org.clp.biznet.Member"
    operation: ALL
    resource: "org.clp.biznet.Partner"
    action: ALLOW
}
```

Member access rules

- Members to have access only to EarnPoints transaction where they are the member

```
rule MemberAccessEarnPoints {
    description: "Allow Member access only to EarnPoints transaction where they
    are the member"
    participant(p): "org.clp.biznet.Member"
    operation: ALL
    resource(r): "org.clp.biznet.EarnPoints"
    condition: (r.member.getIdentifier() === p.getIdentifier())
    action: ALLOW
}
```

Member access rules

- Members to have access only to UsePoints transaction where they are the member

```
rule MemberAccessUsePoints {
    description: "Allow Member access only to UsePoints transaction where they
    are the member"
    participant(p): "org.clp.biznet.Member"
    operation: ALL
    resource(r): "org.clp.biznet.UsePoints"
    condition: (r.member.getIdentifier() === p.getIdentifier())
    action: ALLOW
}
```

Partner access rules

- Partners to have access only to their own account

```
rule PartnerAccessOwnRecord {
    description: "Allow Partner to access only their profile"
    participant(p): "org.clp.biznet.Partner"
    operation: ALL
    resource(r): "org.clp.biznet.Partner"
    condition: (r.getIdentifier() === p.getIdentifier())
    action: ALLOW
}
```

Partner access rules

- Partners Not to have access to other partner accounts

```
rule PartnerAccessPartner {
    description: "Deny Partner access to other Partner accounts"
    participant: "org.clp.biznet.Partner"
    operation: ALL
    resource: "org.clp.biznet.Partner"
    action: DENY
}
```

Partner access rules

- Partners Not to have access to Members on the network

```
rule PartnerAccessMember {
    description: "Deny Partner access to Members on the network"
    participant: "org.clp.biznet.Partner"
    operation: ALL
    resource: "org.clp.biznet.Member"
    action: DENY
}
```

Partner access rules

- Partners to have read access to EarnPoints transaction where they are the partner

```
rule PartnerAccessEarnPoints {
    description: "Allow Partners read only access to EarnPoints transaction
    where they are the partner"
    participant(p): "org.clp.biznet.Partner"
    operation: READ
    resource(r): "org.clp.biznet.EarnPoints"
    condition: (r.partner.getIdentifier() === p.getIdentifier())
    action: ALLOW
}
```

Partner access rules

- Partners to have read access to UsePoints transaction where they are the partner

```
rule PartnerAccessUsePoints {
    description: "Allow Partners read only access to UsePoints transaction where
    they are the partner"
    participant(p): "org.clp.biznet.Partner"
    operation: READ
    resource(r): "org.clp.biznet.UsePoints"
    condition: (r.partner.getIdentifier() === p.getIdentifier())
    action: ALLOW
}
```

THANK YOU!

Any questions?

You can mail us at

hello@blockchain-council.org