// Profile Permissions

rule R1a\_Company\_CanUpdateThemselvesOnly {

description: "Company can see and update their own profile only"

participant(p): "org.capgemeni.sogeti.Company"

operation: READ, UPDATE

resource(r): "org.capgemeni.sogeti.Company"

condition: (r.getIdentifier() == p.getIdentifier())

action: ALLOW

}

//TODO: R1b. Client can view themselves only

//TODO: R1c. Employee can view themselves only

//TODO: R1d. Regulator can view themselves only

// Cross Profile Permissions

rule R2a\_Company\_CanViewTheirEmployees {

description: "Company can view their own employees"

participant(p): "org.capgemeni.sogeti.Company"

operation: READ

resource(r): "org.capgemeni.sogeti.Employee"

condition: ((r.company && r.company.getIdentifier() == p.getIdentifier()) || p.getFullQualifiedType() == "org.capgemeni.sogeti.NetworkAdmin")

action: ALLOW

}

//TODO: R2b. Employee can view their own Company

rule R2c\_Regulator\_CanViewThierCompany {

description: "Regulator can view their Company"

participant(p): "org.capgemeni.sogeti.Regulator"

operation: READ

resource(r): "org.capgemeni.sogeti.Company"

condition: (r.getIdentifier() == p.company.getIdentifier())

action: ALLOW

}

rule R2d\_Regulator\_CanViewTheirCompanyEmployees {

description: "Regulator can view the Company's Employees"

participant(p): "org.capgemeni.sogeti.Regulator"

operation: READ

resource(r): "org.capgemeni.sogeti.Employee"

condition: (p.company.getIdentifier() == r.company.getIdentifier())

action: ALLOW

}

// Consultant Asset Permissions

//TODO: R3a. Company can view their available consultants

rule R3b\_Client\_CanViewUpdateConsultantMarket {

description: "Clients can view/update(via request) available consultants on the market"

participant(p): "org.capgemeni.sogeti.Client"

operation: READ, UPDATE

resource(r): "org.capgemeni.sogeti.Consultant"

condition: (!(r.client))

action: ALLOW

}

rule R3c\_Employee\_CanViewTheirOwnConsultantAsset {

description: "Employee can view their own Consultant asset"

participant(p): "org.capgemeni.sogeti.Employee"

operation: READ

resource(r): "org.capgemeni.sogeti.Consultant"

condition: ((r.employee.getIdentifier() == p.getIdentifier()))

action: ALLOW

}

// SOW Asset permissions

rule R4a\_Company\_CanViewTheirOwnSOWAssets {

description: "Company can view all SOW assets that belong to them"

participant(p): "org.capgemeni.sogeti.Company"

operation: READ, UPDATE

resource(r): "org.capgemeni.sogeti.SOW"

condition: (r.employee.company.getIdentifier() == p.getIdentifier())

action: ALLOW

}

//TODO: R4b. Client can request and view their SOW's

// Transaction Restrictions

rule R5\_Client\_CanRequestConsultantsTxn {

description: "Only clients can requests consultants on the market"

participant: "org.capgemeni.sogeti.Client"

operation: ALL

resource: "org.capgemeni.sogeti.RequestConsultant"

action: ALLOW

}

//TODO: R6. Client can finalize SOW agreement

rule R7\_Company\_CanProposeSOWTxn {

description: "Only company can propose an SOW contract"

participant: "org.capgemeni.sogeti.Company"

operation: ALL

resource: "org.capgemeni.sogeti.ProposeSOW"

action: ALLOW

}

// Historical / Audit Records

rule R8\_Company\_CanViewHistoryOfTheirOwnTransactions{

description: "Company can view their transaction history only"

participant(P): "org.capgemeni.sogeti.Company"

operation: ALL

resource(r): "org.hyperledger.composer.system.HistorianRecord"

condition: (r.participantInvoking.getIdentifier() != p.getIdentifier())

action: DENY

}

rule R8b\_Client\_CanViewHistoryOfTheirOwnTransactions{

description: "Client can view their transaction history only"

participant(P): "org.capgemeni.sogeti.Client"

operation: ALL

resource(r): "org.hyperledger.composer.system.HistorianRecord"

condition: (r.participantInvoking.getIdentifier() != p.getIdentifier())

action: DENY

}

rule R8c\_Employee\_CanViewHistoryOfTheirOwnTransactions{

description: "Employee can view their transaction history only"

participant(P): "org.capgemeni.sogeti.Employee"

operation: ALL

resource(r): "org.hyperledger.composer.system.HistorianRecord"

condition: (r.participantInvoking.getIdentifier() != p.getIdentifier())

action: DENY

}

rule R8d\_Regulator\_CanViewHistoryOfTheirOwnTransactions{

description: "Regulator can view their transaction history only"

participant(P): "org.capgemeni.sogeti.Regulator"

operation: ALL

resource(r): "org.hyperledger.composer.system.HistorianRecord"

condition: (r.participantInvoking.getIdentifier() != p.getIdentifier())

action: DENY

}

// Network/Admin Permissions

rule BizACL {

description: "System ACL to permit all biz access"

participant: "org.hyperledger.composer.system.NetworkAdmin"

operation: ALL

resource: "org.capgemeni.sogeti.\*\*"

action: ALLOW

}

rule SystemACL {

description: "System ACL to permit all access"

participant: "org.hyperledger.composer.system.Participant"

operation: ALL

resource: "org.hyperledger.composer.system.\*\*"

action: ALLOW

}

rule NetworkAdminUser {

description: "Grant business network administrators full access to user resources"

participant: "org.hyperledger.composer.system.NetworkAdmin"

operation: ALL

resource: "org.hyperledger.composer.system.\*\*"

action: ALLOW

}

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

}