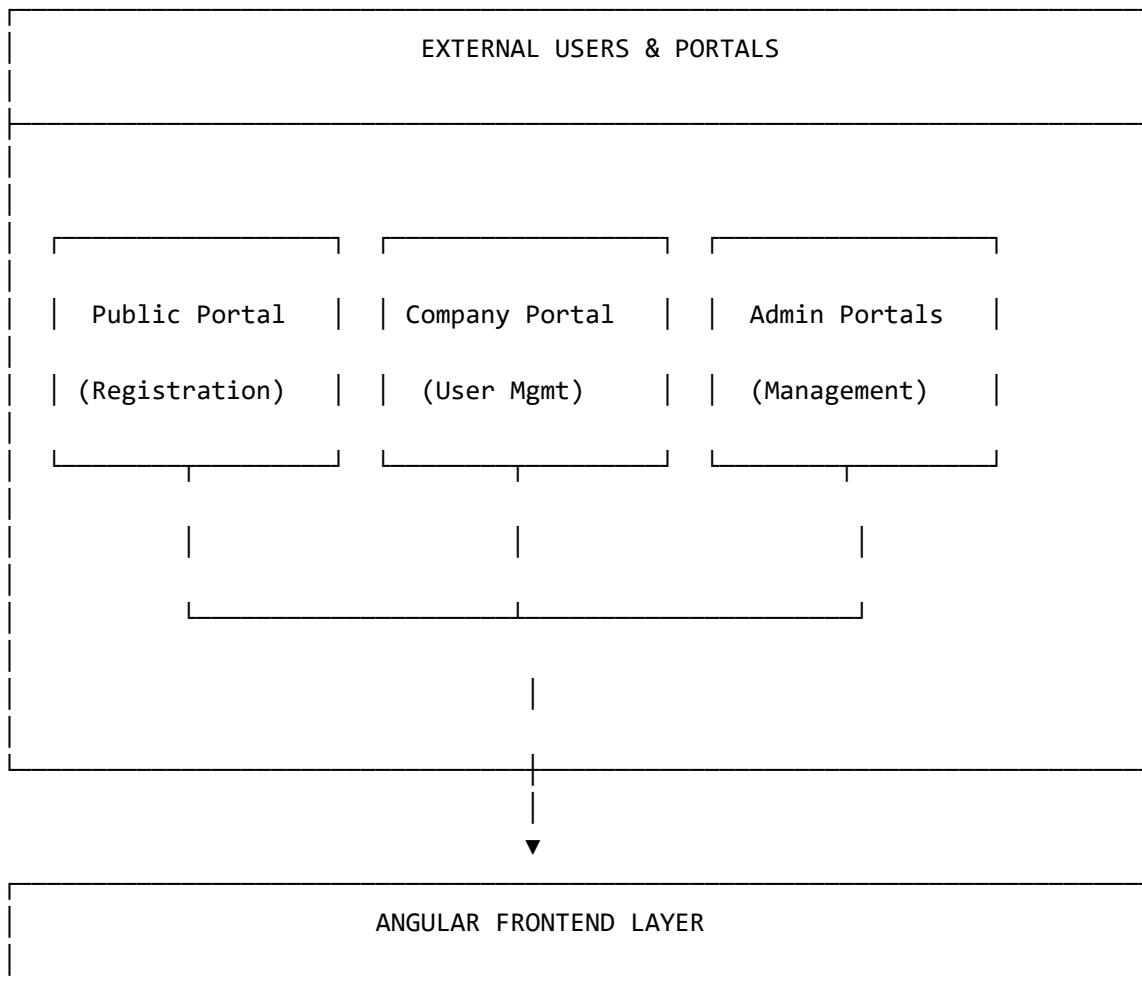
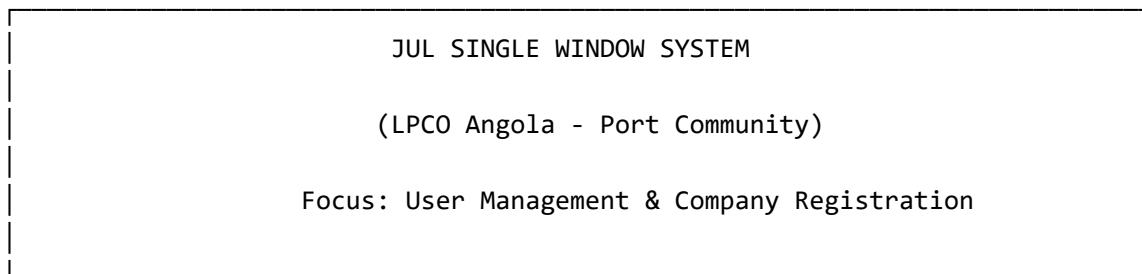
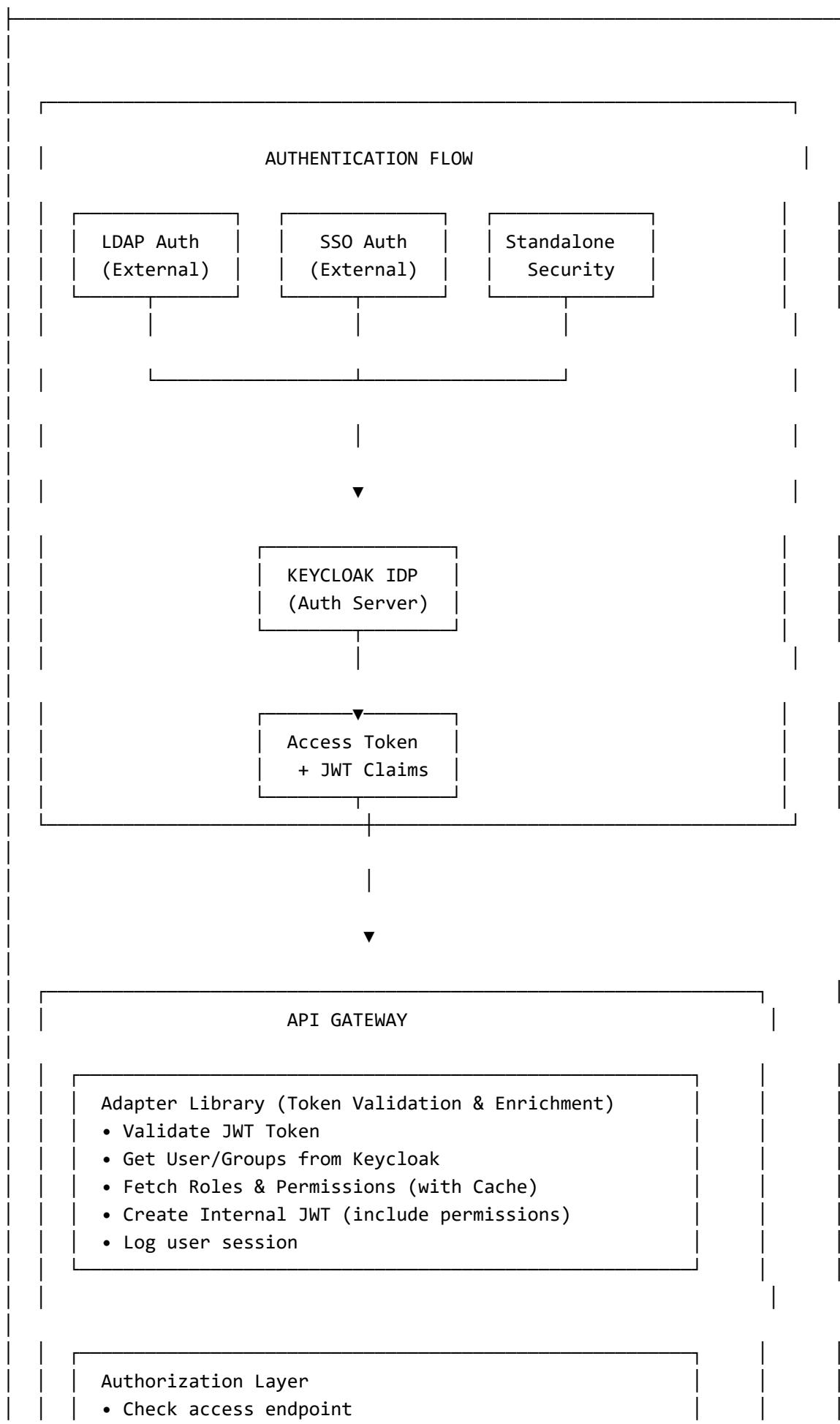


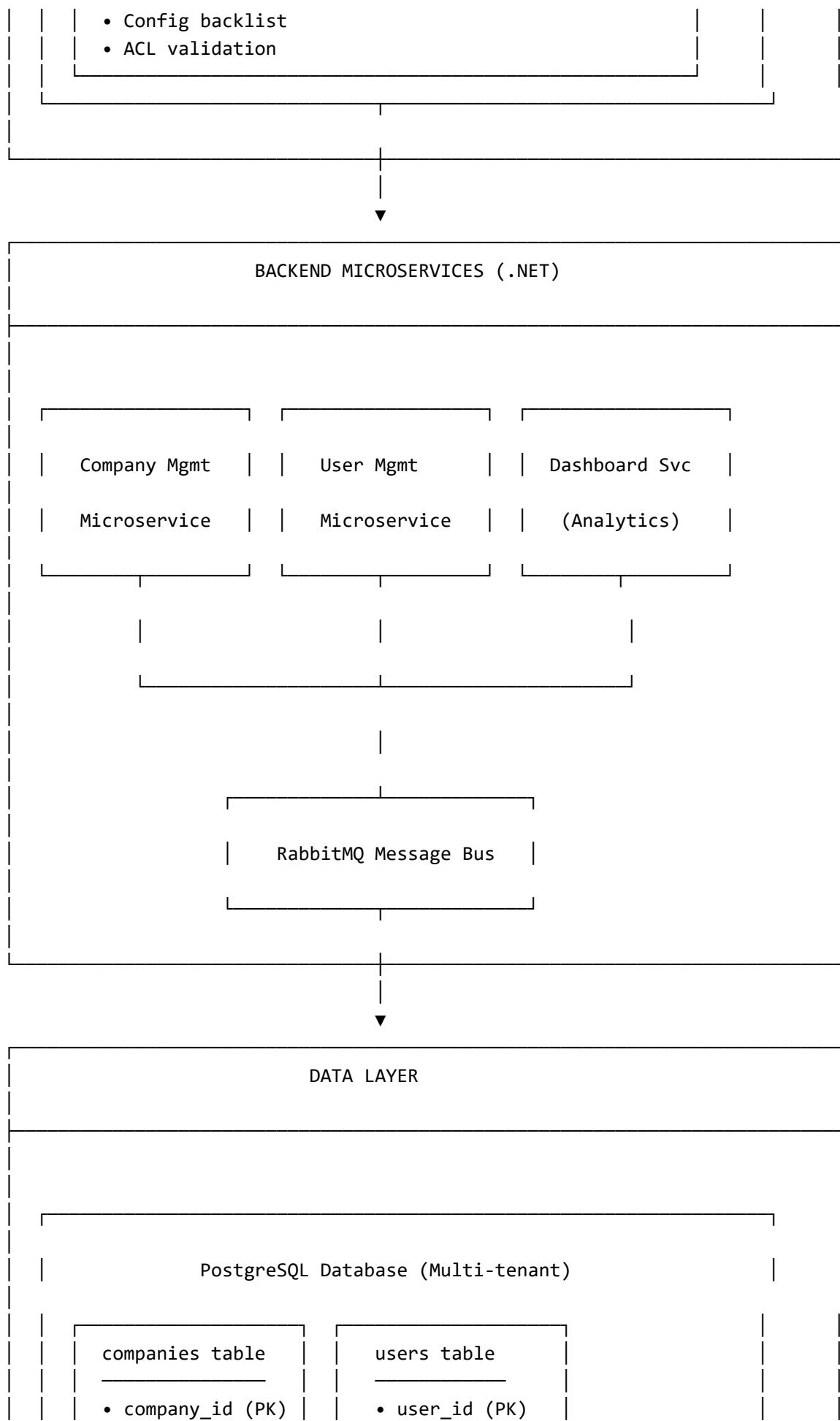
JUL Single Window - System Architecture & Diagrams

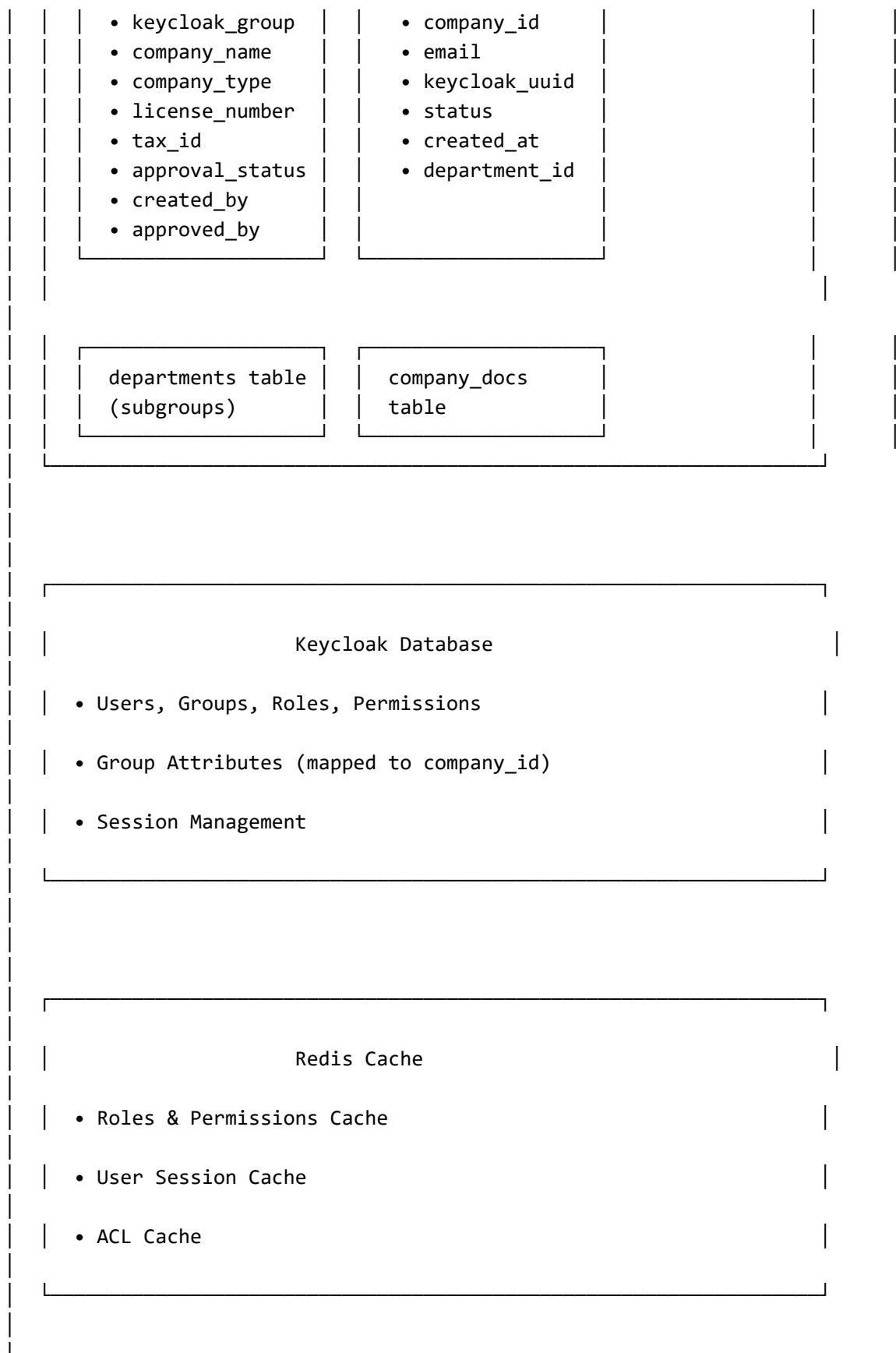
Focus: User Management & Company Registration

1. High-Level System Architecture





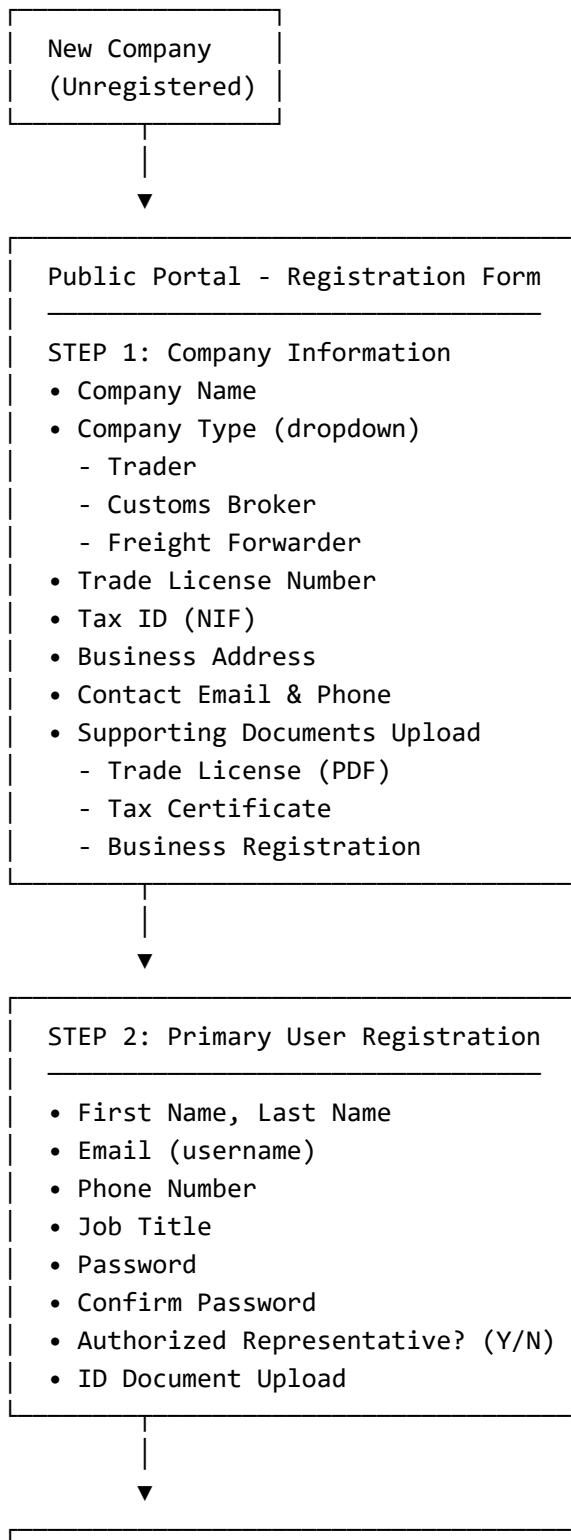


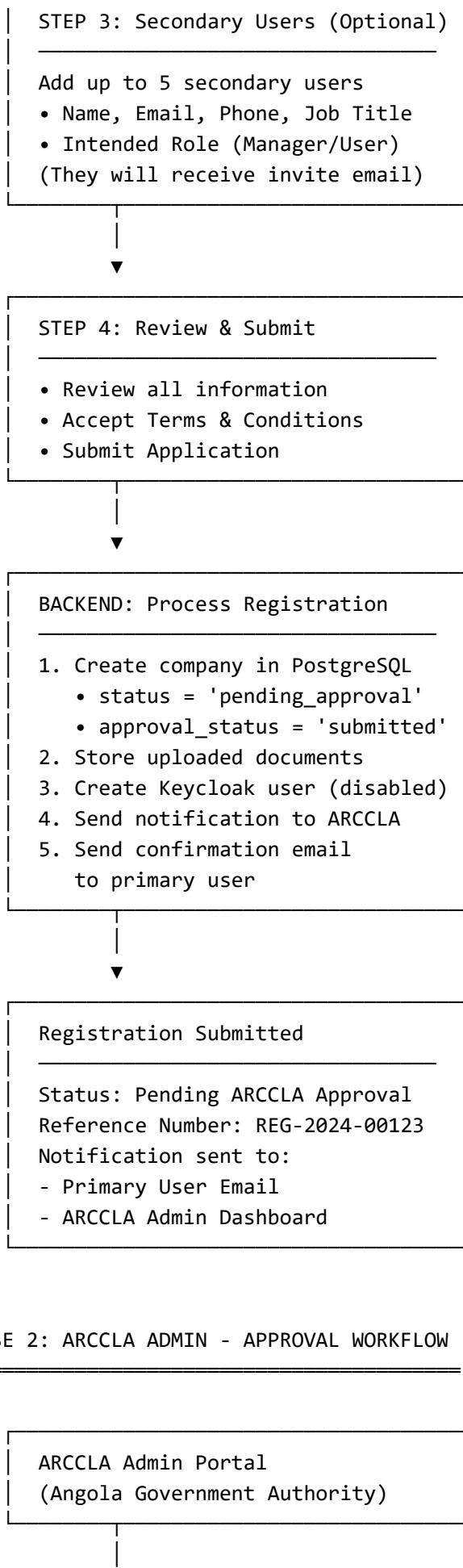


2. Company Registration & User Onboarding Flow

COMPANY REGISTRATION WORKFLOW

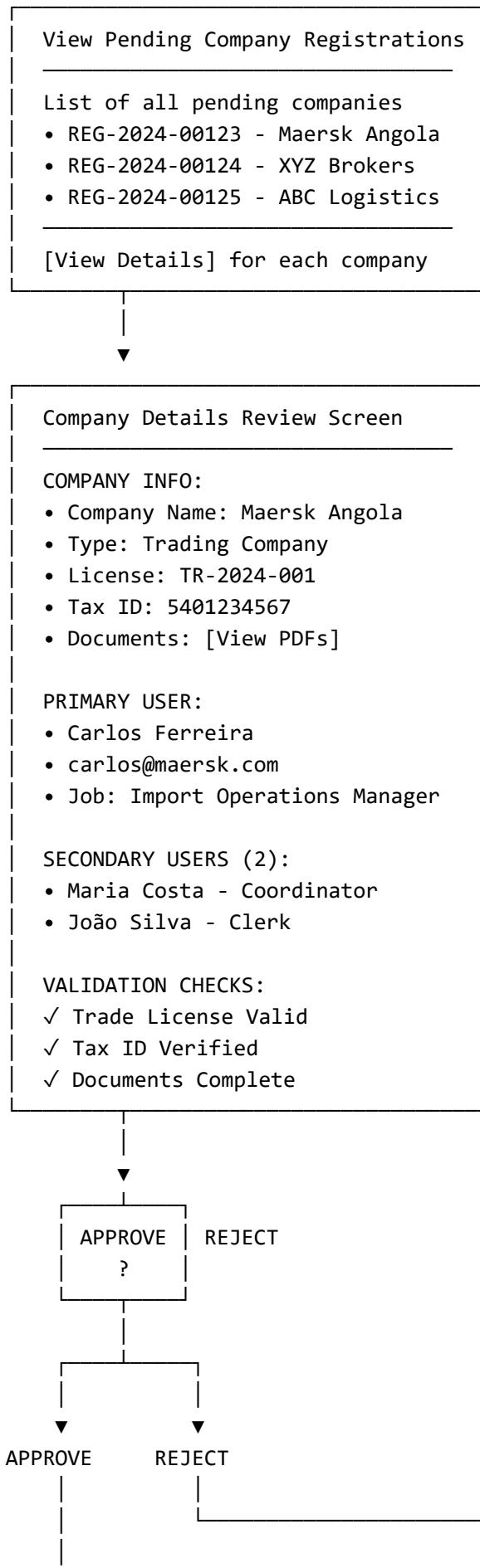
PHASE 1: PUBLIC PORTAL - COMPANY REGISTRATION

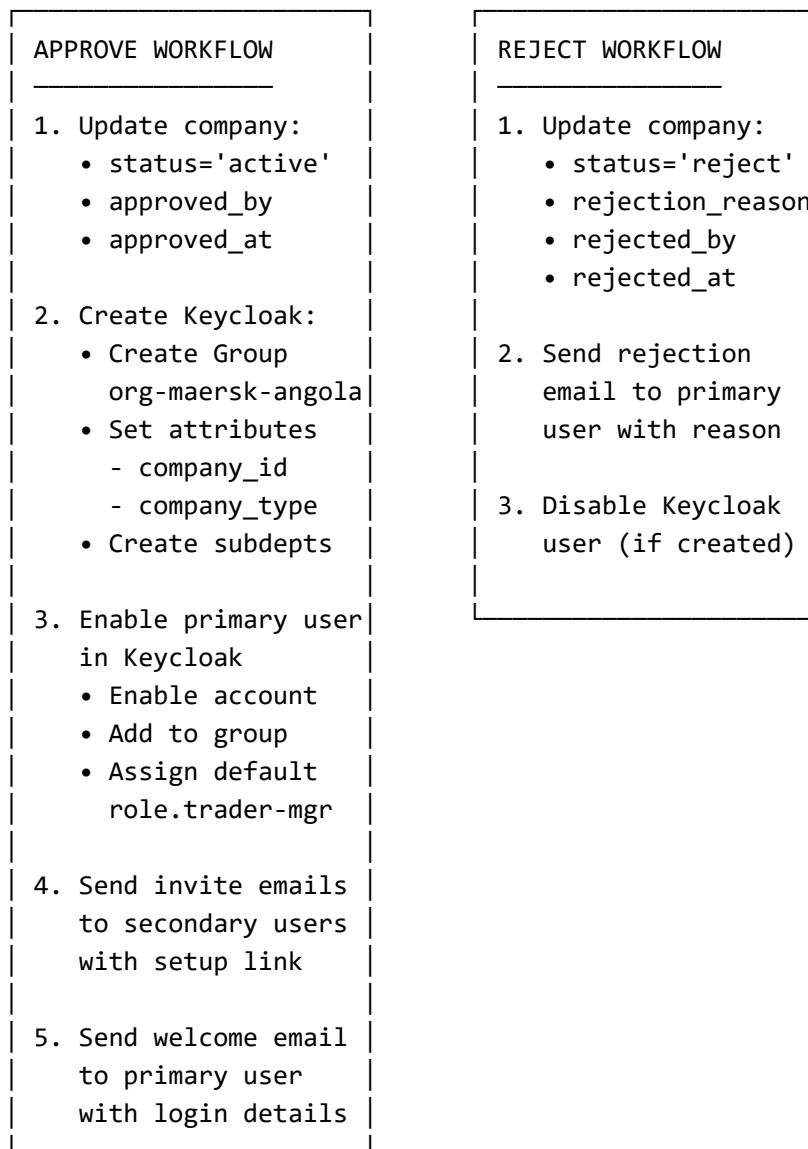




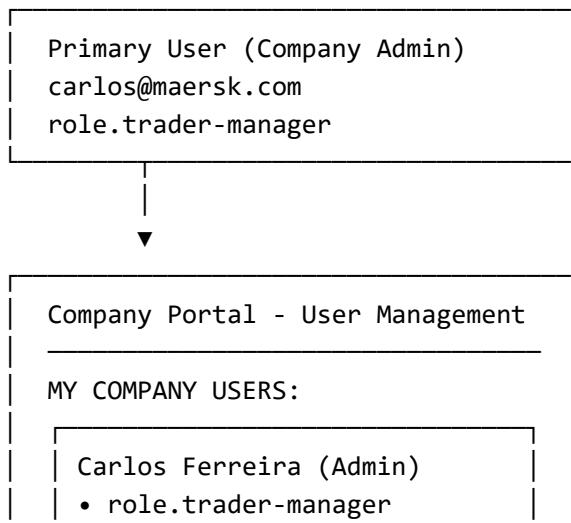
PHASE 2: ARCCLA ADMIN - APPROVAL WORKFLOW

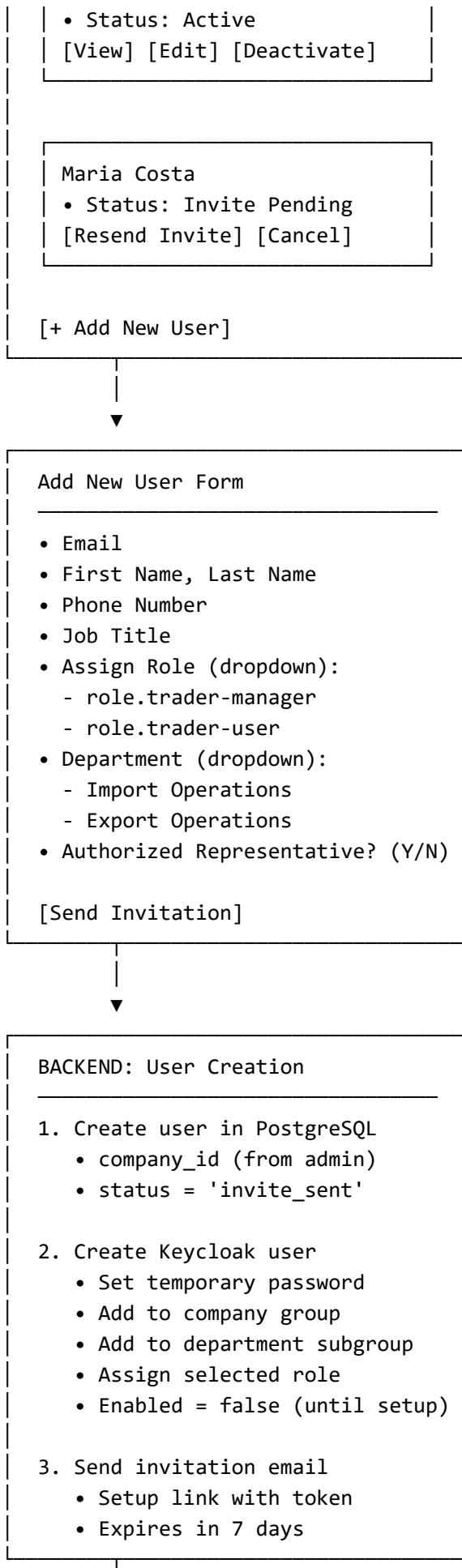
ARCCLA Admin Portal
(Angola Government Authority)





PHASE 3: COMPANY ADMIN - USER MANAGEMENT





|
▼

New User - Account Setup

maria@maersk.com clicks link

1. Verify invitation token
2. Set permanent password
3. Complete profile
4. Accept terms
5. Enable Keycloak account
6. Update status = 'active'
7. Send welcome email

PHASE 4: USER MANAGEMENT OPERATIONS

Company Admin Operations

ACTIVATE USER:

- Enable disabled user account
- Update status in PostgreSQL
- Enable in Keycloak
- Send activation email

DEACTIVATE USER:

- Disable user account
- Update status in PostgreSQL
- Disable in Keycloak
- Revoke active sessions
- Send notification email

EDIT USER:

- Update user details
- Change department
- Update job title
- Modify contact info

ASSIGN ROLES:

- Change user role
- Update in Keycloak
- Invalidate permission cache
- User gets new permissions on next login

VIEW USER ACTIVITY:

- Last login time
- Login history
- Activity logs

3. Admin Portal Structure & Permissions

THREE ADMIN PORTALS

ADMIN 1: SUPER ADMIN (System Administrator)

Role: role.super-admin

Scope: ENTIRE REALM (lpco-angola-system)

RESPONSIBILITIES:

1. KEYCLOAK CONFIGURATION

- Create & manage Realm Roles
 - permission.view, .create, .edit, etc.
- Create & manage Client Roles
 - user-management.*, dashboard.*, etc.
- Create Composite Roles
 - role.trader-manager
 - role.customs-broker-manager
 - role.freight-forwarder-manager
- Configure Client Scopes
- Configure Authentication Flows

2. GROUP TEMPLATES & STRUCTURE

- Define group hierarchy templates
- Set default group attributes schema
- Create department templates

3. SYSTEM CONFIGURATION

- Configure ACL rules
- Manage API Gateway settings

- Configure adapter libraries
- Set up authentication methods
 - LDAP configuration
 - SSO integration

4. MONITORING & AUDIT

- View all system logs
- Monitor user sessions
- Security audit reports
- Performance monitoring

MENU STRUCTURE:

Roles & Permissions

- Realm Roles Management
- Client Roles Management
- Composite Roles Builder
- Permission Matrix View

Groups & Organizations

- Group Templates
- Department Templates
- Attribute Schemas

System Configuration

- Authentication Settings
- API Gateway Config
- ACL Rules Manager
- Adapter Library Settings

Monitoring & Reports

- System Logs
- User Activity
- Security Audit
- Performance Metrics

ADMIN 2: ARCCLA ADMIN (Angola Government Authority)

Role: role.arccla-admin

Scope: ALL COMPANIES (Government Oversight)

RESPONSIBILITIES:**1. COMPANY APPROVALS**

- Review company registrations
- Verify trade licenses
- Validate tax documents
- Approve/Reject companies
- Suspend/Revoke company licenses

2. USER AUTHORIZATION APPROVAL

- Review "Authorized Representative" requests
- Approve signing authority
- Manage authorized user list

3. COMPANY OVERSIGHT

- View all company profiles
- Monitor company users
- View company activity logs

4. COMPLIANCE & CONTROL

- Monitor company activities
- Generate compliance reports
- Manage blacklist/whitelist
- Enforce regulatory policies

MENU STRUCTURE: **Company Management**

- Pending Registrations
- Approved Companies
- Rejected Companies
- Suspended Companies
- Company Details & Documents



ADMIN 3: COMPANY ADMIN (Company User Manager)

Role: role.trader-manager / role.customs-broker-manager /

role.freight-forwarder-manager

Scope: OWN COMPANY ONLY

RESPONSIBILITIES:

1. USER MANAGEMENT (Company Users Only)

- Add new users to company
- Edit user details
- Assign roles to users
 - Can only assign roles within their company type
 - e.g., trader-manager can assign:
 - * role.trader-manager
 - * role.trader-user

- Activate/Deactivate users
- Resend invitation emails
- View user activity logs

2. DEPARTMENT MANAGEMENT

- Create departments (subgroups)
- Assign users to departments
- Manage department structure

3. COMPANY PROFILE

- Update company information
- Manage company documents
- View company statistics

MENU STRUCTURE:

User Management

- All Company Users
- Add New User
- Pending Invitations
- Active Users
- Inactive Users
- User Activity Logs

Department Management

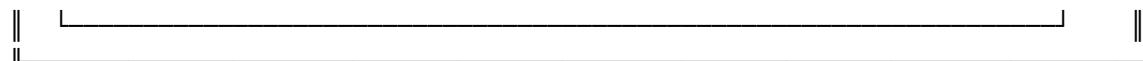
- All Departments
- Create Department
- Assign Users to Departments

Company Dashboard

- Company Statistics
- User Activity Summary
- Recent Notifications

Company Profile

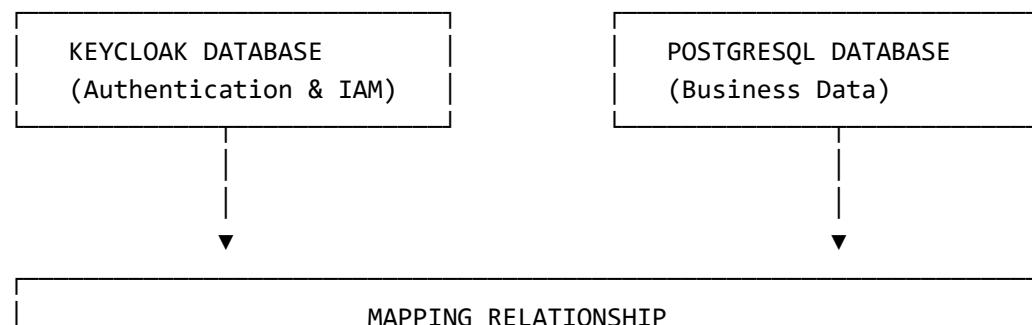
- Company Information
- Update Company Details
- Manage Documents
- Contact Information



4. Keycloak & PostgreSQL Integration

KEYCLOAK & POSTGRESQL INTEGRATION ARCHITECTURE

DATA SYNCHRONIZATION



KEYCLOAK

- Users Table:
 - id (UUID)
 - username (email)
 - firstName
 - lastName
 - enabled
 - attributes
 - phone
 - job_title
 - authorized_to_sign

Groups Table:

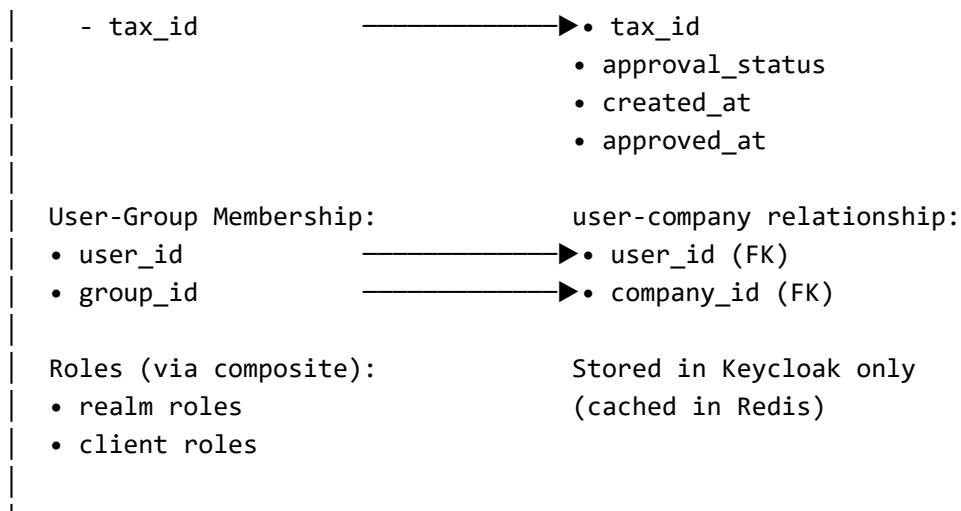
- id (UUID)
- name
 - (org-maersk-angola)
- attributes:
 - org_name
 - org_type
 - company_type
 - license_number

POSTGRESQL

- users table:
 - keycloak_uuid
 - email
 - first_name
 - last_name
 - status (active/inactive)
 - user_attributes (JSONB)
 - phone
 - job_title
 - authorized_to_sign

companies table:

- keycloak_group_id
- company_id (slug)
 - (maersk-angola)
- company_name
 - (Maersk Angola Lda)
- company_type
 - (trading-company)
- license_number



COMPANY CREATION WORKFLOW

WHEN ARCCLA APPROVES A COMPANY:

STEP 1: PostgreSQL Database Update

```

UPDATE companies
SET
    approval_status = 'approved',
    status = 'active',
    approved_by = 'arccla-admin-uuid',
    approved_at = NOW()
WHERE company_id = 'maersk-angola';

```

STEP 2: Keycloak Group Creation via Admin API

```

POST /auth/admin/realms/lpco-angola-system/groups
{
    "name": "org-maersk-angola",
    "attributes": {
        "org_id": ["maersk-angola"],
        "org_type": ["trader"],
        "org_name": ["Maersk Angola Lda"],
        "company_type": ["trading-company"],
        "license_number": ["TR-2024-001"],
        "tax_id": ["5401234567"],
        "status": ["active"],
        "registration_date": ["2024-01-15"],
        "contact_email": ["info@maersk.ao"],
        "contact_phone": ["+244 222 123 456"],
        "address": ["Luanda, Angola"]
    }
}

```

```

        }
    }

Response: { "id": "group-uuid-12345" }

```

STEP 3: Update PostgreSQL with Keycloak Group ID

```

UPDATE companies
SET keycloak_group_id = 'group-uuid-12345'
WHERE company_id = 'maersk-angola';

```

STEP 4: Create Subgroups (Departments)

```
POST /auth/admin/realms/lpco-angola-system/groups/{group-uuid-12345}/children
```

```
{
    "name": "dept-import-operations",
    "attributes": {
        "dept_id": ["maersk-import"],
        "dept_name": ["Import Operations"],
        "dept_code": ["IMP"]
    }
}
```

```
POST /auth/admin/realms/lpco-angola-system/groups/{group-uuid-12345}/children
```

```
{
    "name": "dept-export-operations",
    "attributes": {
        "dept_id": ["maersk-export"],
        "dept_name": ["Export Operations"],
        "dept_code": ["EXP"]
    }
}
```

STEP 5: Enable Primary User & Add to Group

```

// Enable user
PUT /auth/admin/realms/lpco-angola-system/users/{user-uuid}/
{
    "enabled": true
}

// Add user to company group
PUT /auth/admin/realms/lpco-angola-system/users/{user-uuid}/groups/{group-
uuid-12345}

// Assign role
POST /auth/admin/realms/lpco-angola-system/users/{user-uuid}/role-
mappings/realm

```

```
[  
  {  
    "id": "role-trader-manager-uuid",  
    "name": "role.trader-manager"  
  }  
]
```

STEP 6: Update PostgreSQL User Record

```
UPDATE users  
SET  
  status = 'active',  
  company_id = (SELECT id FROM companies WHERE company_id = 'maersk-angola'),  
  activated_at = NOW()  
WHERE keycloak_uuid = 'user-uuid';
```

USER CREATION WORKFLOW (by Company Admin)

WHEN COMPANY ADMIN ADDS A NEW USER:

STEP 1: Create in PostgreSQL First

```
INSERT INTO users (  
  company_id,  
  email,  
  first_name,  
  last_name,  
  phone,  
  job_title,  
  status,  
  created_by,  
  created_at  
) VALUES (  
  (SELECT id FROM companies WHERE company_id = 'maersk-angola'),  
  'maria@maersk.com',  
  'Maria',  
  'Costa',  
  '+244 222 123 002',  
  'Import Coordinator',  
  'invite_sent',  
  'carlos-uuid',  
  NOW()  
)  
RETURNING id, company_id;
```

STEP 2: Create Keycloak User

```
POST /auth/admin/realms/lpco-angola-system/users
{
    "username": "maria@maersk.com",
    "email": "maria@maersk.com",
    "firstName": "Maria",
    "lastName": "Costa",
    "enabled": false, // Will be enabled after setup
    "emailVerified": false,
    "attributes": {
        "phone": ["+244 222 123 002"],
        "job_title": ["Import Coordinator"],
        "company_id": ["maersk-angola"],
        "authorized_to_sign": ["false"],
        "created_by": ["carlos@maersk.com"]
    },
    "credentials": [
        {
            "type": "password",
            "value": "temporary-password-12345",
            "temporary": true
        }
    ]
}
```

Response: { "id": "new-user-uuid-67890" }

STEP 3: Update PostgreSQL with Keycloak UUID

```
UPDATE users
SET keycloak_uuid = 'new-user-uuid-67890'
WHERE email = 'maria@maersk.com';
```

STEP 4: Add User to Company Group

```
PUT /auth/admin/realms/lpco-angola-system/users/new-user-uuid-
67890/groups/group-uuid-12345
```

STEP 5: Assign Role

```
POST /auth/admin/realms/lpco-angola-system/users/new-user-uuid-67890/role-
mappings/realm
[
    {
        "id": "role-trader-user-uuid",
        "name": "role.trader-user"
    }
]
```

STEP 6: Send Invitation Email

```
// Generate invitation token
token = generate_invitation_token(user_id, expires_in_days=7)

// Send email with setup link
send_email({
    to: "maria@maersk.com",
    subject: "Welcome to JUL Single Window",
    body: `
        Hello Maria,

        You have been invited to join Maersk Angola on JUL Single Window.

        Please click the link below to complete your account setup:
        https://jul.angola.gov.ao/setup?token=\${token}

        This link will expire in 7 days.

    `

})
```