DESIGN DOCUMENT

Version 1.0 ● February, 2017

Sougata Maitra

**DESIGN DOCUMENT**

|  |  |
| --- | --- |
| VERSION: 1.0 | REVISION DATE: 22/02/2015 |

Approval of the Technical Architecture indicates an understanding of the purpose and content described in this deliverable. By signing this deliverable, each individual agrees with the content contained in this deliverable.

|  |  |  |  |
| --- | --- | --- | --- |
| **Approver Name** | **Title** | **Signature** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Document Overview 3](#_Toc413095075)

[1.1. Description 3](#_Toc413095076)

[1.2. Scope 3](#_Toc413095077)

[2. Assumed Requirement Overview 3](#_Toc413095078)

[3. Design Details 3](#_Toc413095079)

[3.1. Information Model 3](#_Toc413095080)

[3.2. Entity Descriptions 4](#_Toc413095081)

[3.2.1. State 4](#_Toc413095082)

[3.2.2. District 4](#_Toc413095083)

[3.2.3. Zone 5](#_Toc413095084)

[3.2.4. Village 5](#_Toc413095085)

[3.2.5. Agent 5](#_Toc413095086)

[3.2.6. Role 5](#_Toc413095087)

[3.2.7. User 5](#_Toc413095088)

[3.2.8. Transaction 5](#_Toc413095089)

[3.3. Table Design 6](#_Toc413095090)

[3.3.1. State 6](#_Toc413095091)

[3.3.2. District 6](#_Toc413095092)

[3.3.3. Zone 6](#_Toc413095093)

[3.3.4. Village 7](#_Toc413095094)

[3.3.5. Agent 7](#_Toc413095095)

[3.3.6. Agent Area 8](#_Toc413095096)

[3.3.7. Role 8](#_Toc413095097)

[3.3.8. User 9](#_Toc413095098)

[3.3.9. User Role 9](#_Toc413095099)

[3.3.10. Transaction 9](#_Toc413095100)

[3.4. Sequence Diagram 9](#_Toc413095101)

[3.5. Query Helper 11](#_Toc413095102)

[4. Assumptions 11](#_Toc413095103)

[5. References 11](#_Toc413095104)

# Document Overview

## Description

The client, Senrysa, has a requirement to implement Data Access Control in an application they are building. This document assumes a hierarchical data organization and describes the design for a sample implementation of data access control on it.

The goal of this Design Document is not to serve as a design document for the product Senrysa is building but to provide a sample design which they can implement in the end product to achieve their requirement of data access control.

## Scope

This is a technology agnostic design document and hence does not provide details of technical implementation. It proposes a design with respect to the assumed business scenario/requirements detailed in the next section.

This document covers the design of the data access control but does not go into the domain of role based security and permissions. However, the openness of the proposed design does keep the scope open for this to be integrated in the future.

# Assumed Requirement Overview

A business organization serves a certain geographic area through Agents it appoints in various places. It administers and manages Agents by grouping them under various geographic areas. The region covered by the organization is divided into Zones, States, then Districts and thereafter into Branches. A Zone may have multiple States inside it, a State may have multiple Districts within and each District can have multiple Branches falling under it. Whenever an Agent is appointed, he/she is assigned to one or more areas of operation- the area of operation can be a Zone, State, a District or a Branch. If an Agent is assigned to a State, he/she automatically gets all Branches in that State to be under his/her jurisdiction.

The organization creates two types of Users in its system – ‘*admin*’ and ‘*agent*’. The *admin* type of user will be responsible for creating and managing the master data in the system. The *agent* users will be associated to Agents of the organization. When an Agent logs into the system using his/her user id, he/she will be allowed to only view transaction data related to the villages that fall under his/her jurisdiction. In addition, he/she can perform business operations related to only the villages that fall under his/her jurisdiction.

# Design Details

## Information Model

The following diagram represents the Information Model for the requirement details explained in the preceding section.

Security.wmf

***Figure 1: Information Model***

*Note: The components marked in yellow are part of the LDAP system.*

## Entity Descriptions

The following tables provide a description of the main attributes of each of the entities represented in the Information Model provided in the previous section.

### Zone

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | Zone Identifier | Unique identifier for a Zone in the system |
| 2 | Zone Name | The geographic name of the Zone |
| 3 | Zone Description | System specific description of the Zone, if any |
| 4 | States Covered | List of States that fall under the geographic area of a Zone |

### State

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | State Identifier | Unique identifier for a State in the system |
| 2 | State Name | The geographic name of the State |
| 3 | State Description | System specific description of the State, if any |
| 4 | Districts Covered | List of Districts that fall under the geographic area of a State |

### District

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | District Identifier | Unique identifier for a District in the system |
| 2 | District Name | The geographic name of the District |
| 3 | District Description | System specific description of the District, if any |
| 4 | Branches Covered | List of Branches that fall under the geographic area of a District |

### Branch

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | Branch Identifier | Unique identifier for a Branch in the system |
| 2 | Branch Name | The geographic name of the Branch |
| 3 | Branch Description | System specific description of the Branch, if any |

### Agent

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | Agent Identifier | Unique identifier for an Agent in the system |
| 2 | Agent First Name | First name of the Agent |
| 3 | Agent Last Name | Last name of the Agent |
| 4 | Associated State | The State of jurisdiction of the Agent, if area association is done at State level (multiple associated States possible) |
| 5 | Associated District | The District of jurisdiction of the Agent, if area association is done at District level (multiple associated Districts possible) |
| 6 | Associated Zone | The Zone of jurisdiction of the Agent, if area association is done at Zone level (multiple associated Zones possible) |
| 7 | Associated Branch | The Village of jurisdiction of the Agent, if area association is done at Village level (multiple associated Villages possible) |

### Stakeholder

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | Stakeholder Identifier | Unique identifier for a Stakeholder in the system |
| 2 | Stakeholder Name | Business relevant name of the Stakeholder, e.g. Bank. Corporate BC. |
| 3 | Stakeholder Description | System specific description of the Stakeholder |

### Role

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | Role Identifier | Unique identifier for a Role in the system |
| 2 | Role Name | Business relevant name of the Role |
| 3 | Role Description | System specific description of the Role |
| 4 | Associated Stakeholder | The stakeholder to which the Role logically belongs |

### User

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | User Identifier | Unique identifier for a User in the system |
| 2 | User Name | Name of the User |
| 3 | Associated Role | The role(s) assigned to the User. This is mandatory and multiple Roles may be associated. |
| 4 | Associated Agent | The Agent associated to the User. This is optional (as admin user will not have an associated agent) and maximum one Agent association is allowed. |

### Workflow

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | Workflow Identifier | Unique identifier for a Workflow in the system |
| 2 | Workflow Type | Type of action that is being performed through this workflow. The information will include the entity type being worked upon (e.g. State) and the action being performed (e.g. Add, Modify). |
| 3 | Maker Identifier | The User ID who initiated this workflow |
| 4 | Checker Identifier | The User ID who approved/rejected the workflow |
| 5 | Workflow Status | The current status of the workflow. Possible values are SUBMITTED, APPROVED, REJECTED. |
| 6 | Created On | The date/time when the workflow was initiated |
| 7 | Last Modified On | The date/time when the workflow was last modified |
| 8 | Workflow History | Collection of all state changes of the workflow including comments for each state change |

### Transaction

|  |  |  |
| --- | --- | --- |
| Sl. No. | Attribute Name | Attribute Description |
| 1 | Transaction Identifier | Identifies a business transaction in the system |
| 2 | Agent Identifier | Indicates the Agent associated with the transaction |
| 3 | Village Identifier | Indicates the Village associated with the transaction |

## Table Design

This section describes the required tables, their columns, data types and constraints required to represent the entities described in the preceding sections.

### Zone

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_ZONE | ZONE\_ID |  | Generated Primary Key to identify Zone |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| ZONE\_ID | NUMBER(10) | Unique identifier generated by the system | N | PK\_ZONE |
| ZONE\_NAME | VARCHAR2(50) | Geographic Name | N |  |
| ZONE\_DESC | VARCHAR2(200) | Business Description | Y |  |

### State

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_STATE | STATE\_ID |  | Generated Primary Key to identify State |
| Foreign Key | FK\_ZONE\_STATE | PARENT\_ZONE | ZONE.ZONE\_ID | Parent Zone of a State |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| STATE\_ID | NUMBER(10) | Unique identifier generated by the system | N | PK\_STATE |
| STATE\_NAME | VARCHAR2(50) | Geographic Name | N |  |
| STATE\_DESC | VARCHAR2(200) | Business Description | Y |  |
| PARENT\_ZONE | NUMBER(10) | Zone under which the State falls | N | FK\_ZONE\_STATE |

### District

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_DISTRICT | DISTRICT\_ID |  | Generated Primary Key to identify District |
| Foreign Key | FK\_STATE\_DISTRICT | PARENT\_STATE | STATE.STATE\_ID | Parent state of a district |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| DISTRICT\_ID | NUMBER(10) | Unique identifier generated by the system | N | PK\_DISTRICT |
| DISTRICT\_NAME | VARCHAR2(50) | Geographic Name | N |  |
| DISTRICT\_DESC | VARCHAR2(200) | Business Description | Y |  |
| PARENT\_STATE | NUMBER(10) | State within which the district falls | N | FK\_STATE\_DISTRICT |

### Branch

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_BRANCH | VILLAGE\_ID |  | Generated Primary Key to identify Branch |
| Foreign Key | FK\_DISTRICT\_BRANCH | PARENT\_DISTRICT | DISTRICT.DISTRICT\_ID | Parent District of a Branch |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| BRANCH\_ID | NUMBER(10) | Unique identifier generated by the system | N | PK\_BRANCH |
| BRANCH \_NAME | VARCHAR2(50) | Geographic Name | N |  |
| BRANCH \_DESC | VARCHAR2(200) | Business Description | Y |  |
| PARENT\_DISTRICT | NUMBER(10) | District within which the Branch falls | N | FK\_DISTRICT\_BRANCH |

### Agent

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_AGENT | AGENT\_ID |  | Generated Primary Key to identify Agent |
| Foreign Key |  |  |  |  |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| AGENT\_ID | NUMBER(10) | Unique identifier generated by the system | N | PK\_AGENT |
| AGENT \_NAME | VARCHAR2(50) | Agent’s Name | N |  |
| AGENT\_USER\_ID | VARCHAR2(50) | Login ID in LDAP for the Agent | Y | Refers to User ID existing in LDAP |

### Role

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_ROLE | ROLE\_ID |  | Generated Primary Key to identify Role |
| Foreign Key |  |  |  |  |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| ROLE\_ID | NUMBER(10) | Unique identifier generated by the system | N | PK\_ROLE |
| ROLE\_NAME | VARCHAR2(50) | Business Name of the Role | N |  |
| ROLE\_DESC | VARCHAR2(100) | System specific description of the Role |  |  |
| STAKEHOLDER | VARCHAR2(50) | Identifier of Stakeholder present in LDAP to which the Role belongs |  |  |

### User

There will not be any table modeled in the sample application for User as this will be handled using LDAP. (Please refer Architecture document for details.)

### Stakeholder

There will not be any table modeled in the sample application for associating User to Stakeholder. This will be done in LDAP using the Group attribute to represent the Stakeholder.

### User Role

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_USER\_ROLE | USER\_ID and ROLE\_ID |  |  |
| Foreign Key | FK\_ROLE | ROLE\_ID | ROLE.ROLE\_ID | Role associated to User |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| USER\_ID | NUMBER(10) | Unique identification of User from LDAP | N |  |
| ROLE\_ID | NUMBER(10) | Unique identifier of Role | N | FK\_ROLE |

### User Area

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_USER\_AREA | USER\_ID, ACCESS\_LEVEL\_TYPE and ACCESS\_LEVEL\_VALUE | STATE.STATE\_ID | State to which the Agent is associated |
| Foreign Key |  |  |  |  |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| USER\_ID | NUMBER(10) | Unique identifier from LDAP | N |  |
| ACCESS\_LEVEL\_TYPE | VARCHAR2(50) | Unique identifier of the level of access | N | Possible values are ZONE, STATE, DISTRICT, VILLAGE and ADMIN. |
| ACCESS\_LEVEL\_VALUE | VARCHAR2(50) | Value of Level for which access is allowed | N | ALL is an allowed value for all levels |

### Transaction

This is a table that is used in the sample application to represent business transaction data. The fields mentioned here are assumed to be present in the transaction data of the business system where the data access control will be implemented. *The fields which will be the basis for implementing data access control must be part of such transaction tables in the business system.*

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_TRANS | TRANS\_ID |  | Generated Primary Key to identify the Transaction |
| Foreign Key | FK\_TRANS\_BRANCH |  | BRANCH.BRANCH\_ID | Associated Branch for the transaction |
|  | FK\_TRANS\_AGENT |  | AGENT.AGENT\_ID | Associated Agent for the transaction |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| TRANS\_ID | NUMBER(10) | Unique identifier generated by the system | N | PK\_TRANS |
| TRANS\_BRANCH | NUMBER(10) | Associated Village for the transaction | N | FK\_TRANS\_BRANCH |
| TRANS\_AGENT | NUMBER(10) | Associated Agent for the transaction | N | FK\_TRANS\_AGENT |

### Workflow

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_WORKFLOW | WORKFLOW\_ID |  | Generated Primary Key to identify the Workflow |
| Foreign Key |  |  |  |  |
|  |  |  |  |  |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| WORKFLOW\_ID | NUMBER(10) | Unique identifier generated by the system | N | PK\_WORKFLOW |
| WORKFLOW\_TYPE | VARCHAR2(50) | Type of action performed through the workflow | N | Possible values are ZONE\_ADD, ZONE\_MODIFY etc. |
| MAKER\_ID | VARCHAR2(50) | User who created the workflow | N | Refers to an LDAP User Identifier |
| CHECKER\_ID | VARCHAR2(50) | User who approved/rejected the workflow | Y | Refers to an LDAP User Identifier |
| STATE | VARCHAR2(50) | Current state of the Workflow | N | Possible values are SUBMITTED, APPROVED, REJECTED |
| CREATED\_ON | DATE | Workflow creation date | N |  |
| UPDATED\_ON | DATE | Last modification date | Y |  |

### Workflow History

#### Validations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type | Name | Field | Reference | Description |
| Primary Key | PK\_WORK\_HISTORY | WORKFLOW\_ID and CREATED\_ON |  | Composite primary key of Workflow History |
| Foreign Key |  |  |  |  |
|  |  |  |  |  |

#### Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Field Name | Data Type | Description | Nullable (Y/N) | Reference |
| WORKFLOW\_ID | NUMBER(10) | Unique identifier generated by the system | N |  |
| INITIAL\_STATE | VARCHAR2(50) | The previous state of the workflow | Y | This may be null when a workflow is created for the first time. |
| NEW\_STATE | VARCHAR2(50) | The state the Workflow moved to as part of this action | Y |  |
| MAKER\_ID | VARCHAR2(50) | User who created/resubmitted the workflow | Y | Refers to an LDAP User Identifier |
| CHECKER\_ID | VARCHAR2(50) | User who approved/rejected the workflow | Y | Refers to an LDAP User Identifier |
| COMMENTS | VARCHAR2(300) | Comments added by the user |  |  |
| CREATED\_ON | DATE | The date on which the history entry was created | N |  |

## Sequence Diagram

The following diagram represents the overall sequence of activities that will be performed to implement data access control in a business operation that involves accessing business data.

businessTransaction.wmf

***Figure 2: Sequence diagram for data access control***

Each of the steps in the above diagram is described below.

|  |  |
| --- | --- |
| Step No. | Description |
| 1 | Perform pre-processing steps, if any. (Refer architecture document for details) |
| 2 | The service implemented corresponding to the business operation is triggered from the frontend. |
| 3 | The service forwards the call to the data access layer of the application. |
| 4 | The data access layer determines the query to be triggered. It then passes the query to the helper service (see next section for details), with the additional information of the alias name of the table which contains the Village and Agent identifier along with the index number of the last parameter in the query. |
| 5 | The helper adds additional filter criteria to the query passed in to filter out data not accessible to the particular Agent who is logged in. This filtering is done on the relevant Village and Agent identifiers. The updated query is returned to the data access layer. |
| 6 | The data access layer uses the updated query and triggers it to retrieve data from the database. |
| 7 | The response of the query is returned to the data access layer. |
| 8 | The response is passed on to the calling service. |
| 9 | The queried data is presented to the user via the frontend |
| 10 | Perform post-processing steps, if any. (Refer architecture document for details) |

## Query Helper

The Query Helper, as mentioned in the previous section, provides a service to accept prepared queries and then update them intelligently to ensure, when executed, that data not supposed to be accessible to the logged in user is filtered out.

It does so by executing the following logic:

1. Accept the prepared query, the alias name of the table which contains the columns on which the filtering has to be done, i.e. Village and Agent identifier, and the index number of the last parameter in the query passed in.
2. Retrieve from the session the list of associated Villages for the logged in user/agent.
3. Append into the query two conditions- (a) to match the Agent identifier of the transaction data with the identifier of the logged in Agent, and, (b) to check that the Village identifier of the transaction data falls in the list of associated Villages for the logged in user.
4. Set the values of the Agent and Village identifiers into the updated query.
5. Return the updated query to the caller.

# Assumptions

* When an Agent (who has multiple assigned Villages) logs in to the system, he/she has to choose whether the login should cover ‘*all*’ the allowed Villages or just one. If one, then the specific Village has to be chosen. Thereafter, all data access control processing is done based on that Village. The business processes triggered by the user, if any, are also done in context of that chosen Village. If the user chooses ‘All’, then the data for all associated Villages is made accessible. On trying to do some business processing, the user is then allowed to choose one of the allowed Villages as the context in which the business process is being executed.
* Each and every transaction happening in the system will be in relation to a certain Village and an Agent. Hence, each transaction data will have an associated Village and Agent identifier.
* The column names and data types of the Village and Agent identifiers in all transaction tables will always be the same.

# References

Architecture document.