SERVICE REQUEST 10205:
APPLICATION RESOURCE
SECURITY MANAGER (ARSM)
DETAILED DESIGN
RELEASE 656

April 27th, 1992

Information Systems & Computing
Office of the President
University of California

final
# Table of Contents

- **Introduction** ........................................... 1
- **Service Request 10205** ................................ 1
- **Differences from Requirements Definition** ........... 2

**ARSM Function Codes** .................................... 3

- **DDL** ..................................................... 4
  - TBHAC00C .................................................. 4
  - IXHAC00C .................................................. 4
  - IXHA200C .................................................. 4
  - TSHAC00C .................................................. 4
  - UC0VHAC1 .................................................. 4
  - PPPVZHAC .................................................. 4

- **Include** .................................................. 5
  - UC0VHAC1 .................................................. 5
  - PPPVZHAC .................................................. 5

- **Copymembers** ........................................... 6
  - UCWSCOMA .................................................. 6
  - UCWSCOMN .................................................. 6

**Programs** .................................................. 7

- **UCPPEDB** .................................................. 7
  - Hierarchical Access Rule .................................. 7
  - Home Department Range Rule .............................. 7
  - Personnel Program Rule .................................. 7
  - Student Status Rule ..................................... 8

- **UCWEASC** .................................................. 8
- **UCWEGRP** .................................................. 9
- **UCWARSM** .................................................. 9
- **UCARSMRP** .................................................. 9
- **UCWERUL** .................................................. 9
- **UCWEACC** .................................................. 9
- **UCWEHAP** .................................................. 10
- **UCWEHAS** .................................................. 10
- **UCWERNG** .................................................. 10
- **UCERNG0** .................................................. 10
- **UCWEHME** .................................................. 10
- **UCEHME0** .................................................. 11
- **UCWEDST** .................................................. 11
- **UCEDST0** .................................................. 11
- **UCEASC0** .................................................. 12
- **UCARSM0** .................................................. 12
- **UCEHAP0** .................................................. 13
- **UCEHAS0** .................................................. 13
Introduction

A requirement of the Payroll/Personnel On-line System security was to provide a means of restricting a user's access to employee records to a subset of the entire record population. The Application Resource Security Manager (ARSM) was developed to satisfy this requirement. The conceptual design of ARSM is as follows:

- Enable campuses without local security mechanisms to carry out population selection controls in the Payroll/Personnel On-line System;
- Provide the framework for implementing expanded local security requirements on Payroll/Personnel data;
- Provide a generalized resource security manager for use with other campus applications systems.

Presently, ARSM controls access to application data by Group, Rule, Access and Association Tables. The Group Table allows users to be grouped together so that rules can be established for the entire group rather than each individual user. Both individual user ID's and Group ID's are referred to as Authorization ID's. A user can be a member of more than one group. The Rule Table is used to identify a rule, e.g., HMEDPT, the resource to which the rule controls access, and the relative priority of that rule. The Access Table actually connects a user or group of users to a specific rule for a specific resource. For example, the Access Table establishes for PAYGRP1 a HMEDPT rule for accessing EDB data. The Association Table contains specific data values needed by certain Access Rules (EDB Range, Home Department, Distribution Department).

The specific access types are Universal, Employee ID Range, Home Department and Distribution Department access rules. Universal access is where all records of a set of data are accessible. The Employee ID Range accessibility is determined by a range of employee identification numbers associated with an Authorization ID. The Home Department and Distribution Department Access types are based on Department codes associated with an Authorization ID.

The screens used to update the Group, Rule, Access and Association tables require the input and update of each table for each Authorization ID.

Service Request 10205

Payroll Coordination requests that ARSM provide a means of further restricting a user's access to employee records to a subset of the entire population.

It is requested that ARSM be modified to include a Hierarchical Organization Model. This model should allow campuses to control access to employee records by a hierarchy of the user population including Central Administrative, Deans/Business/Vice Chancellor, and Departmental Offices.

It is desired that the following elements be used in constructing a Hierarchical Model:

1. Utilization of a table concept that can be easily maintained and can accept mass transactions;
2. Provide some function supporting on-line updating of the new tables(s);

In addition to the Hierarchical Model two new rules will be added to ARSM:

1. Determine record accessibility by specific Personnel Program Code;
2. Determine record accessibility by ranges of Home Department Codes.
This document specifies the changes needed to modify the Application Resource Security Manager in satisfaction of service request 10205.

**Differences from Requirements Definition**

The following are clarifications to, or differences from, the requirements definition which are necessary to allow implementation of the requirements in Application Resource Security Manager.

- It has been requested that three additional ARSM screens be developed:
  - one screen to facilitate updating and/or adding all types of association data, to replace the existing four screens (1 menu and 3 detail screens);
  - two screens to facilitate updating and/or adding entries to the hierarchical table.
- The following requirement was added to Service Request 10205:
  - Add a new rule to determine record accessibility by specific Student Status types.
- The following requirements were removed from Service Request 10205:
  - Expansion of the Range Access Rule to include Personnel Program Codes;
  - Inclusion of security which would not allow a user to update his/her own record;
  - **Note**: that the requirement to prevent a user from updating his/her records will be addressed during the requirements definition phase of EDB Entry/Update.
  - Allow the access to employee records from one department/unit by another department/unit.
  - **Note**: this requirement is presently satisfied by the conjunctive rule.
ARSM Function Codes

Two new ARSM function codes EHAP, Primary Unit Maintenance and EHAS, Secondary Unit Maintenance will be established to perform Hierarchy Table Maintenance.

The ARSM function code EASC will be modified so that when entered the Association Maintenance screen will be presented instead of the Association Maintenance Menu screen (which will become obsolete with these modifications).

ARSM function codes ERNG, EHME and EDST will become obsolete with these modifications.
DDL

TBHAC00C
This new DDL member will contain the SQL statements necessary to create DB2 table UC0HAC. The table will be defined as follows:

    PRIMARY_UNIT  CHAR(06) NOT NULL
    SECONDARY_UNIT CHAR(06) NOT NULL
    PRIMARY KEY (PRIMARY_UNIT, SECONDARY_UNIT)

Each table row will contain an entry for a primary unit and a secondary unit it is allowed to access. A table row will exist for each secondary unit the primary unit is allowed to access.

IXHAC00C
This new DDL member will contain the SQL statements necessary to create the index for Hierarchy Access Table UC0HAC in primary unit sequence.

IXHA200C
This new DDL member will contain the SQL statements necessary to create the index for Hierarchy Access Table UC0HAC in secondary unit sequence.

TSHAC00C
This new DDL member will contain the SQL statements necessary to create the tablespace for Hierarchy Access Table UC0HAC.

UC0VHAC1
This new DDL member will contain the SQL statements necessary to create view UC0VHAC1_HAC of Hierarchy Access Table UC0HAC.

PPPVZHAC
This new DDL member will contain the SQL statements necessary to create view PPPVZHAC_HAC of Hierarchy Access Table UC0HAC.
Include

UC0VHAC1

This new include member will contain the SQL statements necessary to create view UC0VHAC1_HAC of Hierarchy Table UC0HAC.

PPPVZHAC

This new include member will contain the SQL statements necessary to create view PPPVZHAC_HAC of Hierarchy Table UC0HAC.
Copymembers

UCWSCOMA
This copymember will be modified to add the working storage variables needed to evaluate variable rule names and ranges of data.

UCWSCOMN
This copymember will be modified to remove the EDB Range, Home Department and Distribution Department working storage variables. The Hierarchical working storage variables will also be added.
Programs

**UCPPPDEDB**

This program needs to be modified to process each access rule. Modifications for each rule are as follows:

**Hierarchical Access Rule**

This rule obtains the Primary Unit and Secondary for the Hierarchy Access Table and determines if the user is allowed access to requested information based on the user’s Association Data.

This rule is created as follows.

- Declare Hierarchy Cursor, select the secondary unit from the Hierarchy Table where the primary unit is greater than or equal to the association data beginning range value and the primary unit is less than or equal the association data ending range value.
- Create Working Storage field called WS-HACRNG-VALUE;
- Modify 2100-GET-ASSOC-DATA to check for this rule;
- Create a processing paragraph 2150-CHECK-HACRNG-DATA similar to 2120-CHECK-DISDPT-DATA;

**Home Department Range Rule**

This rule obtains the Home Department code from the Personnel Table and determines if the user is allowed access to requested information based on the user’s Association Data.

This rule is created as follows.

- Create Working Storage field called WS-HMERNG-VALUE;
- Modify 2100-GET-ASSOC-DATA to check for this rule;
- Create a processing paragraph 2140-CHECK-HMERNG-DATA similar to 2120-CHECK-DISDPT-DATA;

**Personnel Program Rule**

This rule obtains the Personnel Program field from the Appointment Table and determines if the user is allowed access to requested information based on the user’s Association Data.
This rule is created as follows:

- Create a one-byte Working Storage field called WS-PERSONNEL-PGM;
- Modify 2100-GET-ASSOC-DATA to check for this rule;
- Create a processing paragraph 2160-CHECK-PERPGM-DATA similar to 2120-CHECK-DISDPT-DATA;
- Declare the PERPGM_CURS like the DIST_CURS.
- Add code to select the PERSONNEL_PGM into corresponding working storage field. This select will be performed for every Personnel Program Code from all appointments for the employee until a match is found or all appointments have been searched.

**Student Status Rule**

This rule obtains the Student Status field from the Personnel Table and determines if the user is allowed access to requested information based on the user's Association Data.

This rule is created as follows:

- Create a one-byte Working Storage field called WS-STUDENT-STATUS;
- Expand the select in paragraph 8300-SLCT-PERS to additionally select STUDENT_STATUS into WS-STUDENT-STATUS;
- Modify the 2100-GET-ASSOC-DATA paragraph to accept this new rule;
- Create a processing paragraph 2170-CHECK-STUSTA-DATA similar to 2120-CHECK-DISDPT-DATA.

**UCWEASC**

This program needs to be modified so that function code EASC presents the new entry/update screen which combines the functions of ERNG, EHME and EDST.

This program will be modified to accept the values for the EDB Range, Home Department or Distribution Department rules directly from the new Association Maintenance entry/update screen.

Obsolete transactions ERNG, EHME and EDST will be removed from paragraph 4130-EDIT-FUNC. The EHTM, Hierarchy Table Maintenance transaction will be add to this paragraph.

**Error Report 766**

The original design of ARSM specified that multiple association rows could be linked to an access rule. For example, a user could be allowed to access EDB records with two different Home Department Codes. This requires that two association rows, one for each Home Department Code, be established. The Association table (UC0ASC) has a column SEQ_NUMBER which allows multiple rows for the same IDENTIFIER and ACCESSRULE. However, programs UCWEHME and UCWEDST always move ‘1’ to the SEQ_NUMBER which prevents more than one association rule for the Identifier Access Rule Combination. UCWEASC will be modified to allow multiple association rows, by locating the highest sequence number and incrementing it for each add.
**UCWEGRP**

Obsolete transactions ERNG, EHME and EDST will be removed from paragraph 4130-EDIT-FUNC. The EHAP and EHAS, Hierarchy Table Maintenance transactions will be add to this paragraph.

**UCWARSM**

Obsolete transactions ERNG, EHME and EDST will be removed from paragraph 4130-EDIT-FUNC. The EHAP and EHAS, Hierarchy Table Maintenance transactions will be add to this paragraph.

**UCARSMRP**

*Error Report 745*

Modifications will be made so that the following errors in program UCARSMRP will be fixed:

- When more than one report is requested, only the first report starts with page one. All other reports start with a page number after the last page of the previous report.
- On all pages except the first page of all reports, the second line (all dashes) is repeated and a detail line is missing.
- When reporting on rules, the program uses SQL to JOIN the Access Table (UC0ACC) and the Association Table (UC0ASC). Not all Access rules need Association data (e.g., UNIVERSAL rules). The result is that no universal rules are reported.

**UCWERUL**

Obsolete transactions ERNG, EHME and EDST will be removed from paragraph 4130-EDIT-FUNC. The EHAP and EHAS, Hierarchy Table Maintenance transactions will be add to this paragraph.

**UCWEACC**

Obsolete transactions ERNG, EHME and EDST will be removed from paragraph 4130-EDIT-FUNC. The EHAP and EHAS, Hierarchy Table Maintenance transactions will be add to this paragraph.

*Error Report 745*

Modifications will be made so that the following errors in program UCWEACC will be fixed:

- The on-line ARSM Access Rule Maintenance screen (EACC) allows the user to change the Access Rule name. This causes a problem because Access Rule is part of the primary key of the Access table (UC0ACC). When the program attempts to update the row, a SQLCODE of +100 is returned. The program abends because there is no code to handle a SQLCODE of +100.
The program will be modified to:

- prohibit the change of any field that is part of the key;
- perform a DELETE and then a INSERT in order to change the Access Rule name.

**UCWEHAP**

This new program will be added to ARSM to populate and maintain the Hierarchy Access Table in primary unit sequence. This program will read the Hierarchy DB2 Table and create all one to one corresponding rows on the Hierarchy Access Table needed by ARSM to determine departmental hierarchical access.

The primary unit and each secondary unit will be entered on the Hierarchy Table Maintenance Screen, UCEHAP0.

Program UCWEHAP will display the UCEHAP0 screen, collect entered data, process the addition or deletion of each table row in primary unit sequence.

The user displays the screen by entering the function code EHAP on the Command Line of any ARSM System Administration screen to display the Hierarchy Table Maintenance screen.

**UCWEHAS**

This new program will be added to ARSM to populate and maintain the Hierarchy Access Table in secondary unit sequence. This program will read the Hierarchy DB2 Table and create all one to one corresponding rows on the Hierarchy Access Table needed by ARSM to determine departmental hierarchical access.

The secondary unit and each primary unit will be entered on the Hierarchy Table Maintenance Screen, UCEHAS0.

Program UCWEHAS will display the UCEHAS0 screen, collect entered data, process the addition or deletion of each table row in secondary unit sequence.

The user displays the screen by entering the function code EHAP on the Command Line of any ARSM System Administration screen to display the Hierarchy Table Maintenance screen.

**UCWERNG**

This program will become obsolete after these modifications have been released.

**UCERNG0**

This map will become obsolete after these modifications have been released.

**UCWEHME**

This program will become obsolete after these modifications have been released.
**UCEHME0**
This map will become obsolete after these modifications have been released.

**UCWEDST**
This program will become obsolete after these modifications have been released.

**UCEDST0**
This map will become obsolete after these modifications have been released.
UCEASC0

This map will be converted from a Menu screen to an Entry/Update screen. The following rules may be established on this screen EDB Range, Home Department and Distribution Department.

The Personnel Program Code and the Student Status may be entered on this screen as association data.

The valid EDB Range values are Employee Id and Home Department Codes.

<table>
<thead>
<tr>
<th>UCEASC0-E0656</th>
<th>Application Resource Security Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Association Maintenance</td>
</tr>
<tr>
<td>A/D/C</td>
<td></td>
</tr>
<tr>
<td>Rule Name</td>
<td></td>
</tr>
<tr>
<td>Identifier</td>
<td></td>
</tr>
<tr>
<td>Range-Value1</td>
<td>Range-Value2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PF: 2-Cancel  3-Prevmenu  9-Mainmenu  12-Exit

UCARSMO

This map will be modified to add the EHAP and EHAS, Hierarchy Table Maintenance function codes.

<table>
<thead>
<tr>
<th>UCARSMO-M0656</th>
<th>Application Resource Security Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Main Menu</td>
</tr>
<tr>
<td></td>
<td>Userid: ...</td>
</tr>
</tbody>
</table>

. EGRP Group Maintenance
. ERUL Rule Maintenance
. EACC Access Maintenance
. EASC Association Maintenance
. EHAP Hierarchy Primary Unit Maintenance
. EHAS Hierarchy Secondary Unit Maintenance

PF: 12-Exit

Programs
**UCEHAP0**

This map will be created to present the Hierarchy Table Maintenance screen.

<table>
<thead>
<tr>
<th>UCEHAP0-E0656</th>
<th>Application Resource Security Manager</th>
<th>...........</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hierarchy Maintenance - Primary Unit</td>
<td>Userid:</td>
</tr>
<tr>
<td>Primary Unit:</td>
<td>...........</td>
<td>2-Cancel</td>
</tr>
<tr>
<td>Secondary Units:</td>
<td>...........</td>
<td>9-Mainmenu</td>
</tr>
</tbody>
</table>

**UCEHAS0**

This map will be created to present the Hierarchy Table Maintenance screen.

<table>
<thead>
<tr>
<th>UCEHAS0-E0656</th>
<th>Application Resource Security Manager</th>
<th>...........</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hierarchy Maintenance-Secondary Unit</td>
<td>Userid:</td>
</tr>
<tr>
<td>Secondary Unit:</td>
<td>...........</td>
<td>2-Cancel</td>
</tr>
<tr>
<td>Primary Units:</td>
<td>...........</td>
<td>9-Mainmenu</td>
</tr>
</tbody>
</table>