South Dakota Board of Regents
Modification Id: SDBOR 003
Distributed Banner Form-Object
Security
General
Functional Specification

Prepared by: Melissa Shearer
Version: 3.0
Last Revision Date: 03/31/2006
Create Date: 03/19/2006

Project Manager: Melissa Shearer
Functional Consultant Lead: Melissa Shearer
Technical Consultant Lead: Bill Lee
Table of Contents

1 DISTRIBUTED BANNER FORM-OBJECT SECURITY ........................................ 5
   1.1 INTRODUCTION .................................................................................. 5
   1.2 OVERVIEW ....................................................................................... 5
   1.3 SCOPE .............................................................................................. 5
       1.3.1 Product Release ......................................................................... 5
       1.3.2 Assumptions .............................................................................. 5
       1.3.3 Exclusions .................................................................................. 7
       1.3.4 Concerns ..................................................................................... 7
       1.3.5 Terminology ............................................................................... 7
       1.3.6 Security ........................................................................................ 7
       1.3.7 Site Policy Impact ...................................................................... 7
   1.4 FUNCTIONALITY .................................................................................. 7
       1.4.1 Functional Process Flow ............................................................. 7
       1.4.2 New Human Computer Interactions (HCI)/Forms ..................... 9
       1.4.3 Modified Human Computer Interactions (HCI)/Forms ............. 10
       1.4.4 New Web Applications ............................................................... 10
       1.4.5 Modified Web Applications ....................................................... 10
       1.4.6 New Processes ............................................................................ 10
       1.4.7 Modified Processes ..................................................................... 10
       1.4.8 New Reports ............................................................................... 10
       1.4.9 Modified Reports ........................................................................ 10
       1.4.10 New Reporting Structures ......................................................... 10
       1.4.11 Modified Reporting Structures .................................................. 10
   1.5 DATABASE ......................................................................................... 10
       1.5.1 New Tables .................................................................................. 10
       1.5.2 Modified Tables .......................................................................... 11
       1.5.3 New Views .................................................................................. 14
       1.5.4 Modified Views ........................................................................... 14
       1.5.5 New Functions ............................................................................. 14
       1.5.6 Modified Functions .................................................................... 14
       1.5.7 New Procedures .......................................................................... 14
       1.5.8 Modified Procedures .................................................................. 14
       1.5.9 New Packages ............................................................................. 14
       1.5.10 Modified Packages .................................................................... 15
       1.5.11 New Other .................................................................................. 15
       1.5.12 Modified Other ........................................................................... 15

2 CROSS ENTERPRISE CONSIDERATIONS .................................................. 15
   2.1.1 Campus Pipeline/Luminis ............................................................... 15
   2.1.2 SunGard SCT Workflow Examples .............................................. 15
   2.1.3 WebCT Interface Processes ......................................................... 15
   2.1.4 Learning Systems .......................................................................... 15
   2.1.5 Other Interfaced Systems .............................................................. 15

3 CONTRACT INFORMATION ................................................................. 15
<table>
<thead>
<tr>
<th></th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>APPROVAL TO PROCEED</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>DOCUMENT HISTORY</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>ACRONYMS</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>DEFINITIONS</td>
<td>19</td>
</tr>
</tbody>
</table>
1 Distributed Banner Form-Object Security

1.1 Introduction

This functional specification document represents the outcome of an iterative review process. It is considered a product-planning document and does not represent a commitment to develop the described software changes in the manner presented. SunGard SCT reserves the exclusive right to determine, in its sole discretion, the enhancements to be developed by SunGard SCT and the manner in which they are developed.

1.2 Overview

The South Dakota Board of Regents is made up of six universities, two special schools and a central Board of Regents office. They are implementing the Banner administrative system for multiple campuses but they do not use a VPD’d environment. Some security functions for the Banner system are performed by the central Board of Regents staff (hereafter referred to as RIS) and some security functions will be performed at individual campuses by University Security Coordinators (hereafter referred to as USC).

The RIS staff will utilize the Banner security user id (BANSECR) for forms and objects as delivered by baseline. However, they wish to customize Banner distributed security for the USC's so that there are limited functions that the USC's can perform based upon their login security IDs.

This customization will establish Fine Grained Access Control (FGAC) policies on the security tables that will enable or restrict the ability of an individual security user to either query, update, insert or delete records based upon a comparison of their login to the established policies.

1.3 Scope

1.3.1 Product Release

<table>
<thead>
<tr>
<th>Module</th>
<th>Release Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SunGard Higher Education Banner® General</td>
<td>7.2</td>
</tr>
</tbody>
</table>

1.3.2 Assumptions

1. All customizations will be developed and delivered in SCT Banner® General 7.2.
2. Objects not mentioned in this Specification are outside the scope of the proposed solution. Any change in scope will be handled with a Change Request and a re-evaluation of effort.

3. SunGard Higher Education will deliver efficient, well-formed code, analyzed for optimal performance according to Oracle and SunGard Higher Education standards.

4. A single point of contact from the Client will be identified for communication during the project. This single point of contact will be responsible for all communication with SunGard Higher Education, including the review and approval of project deliverables and formal acceptance of the final product.

Client approval will be required on the following documents:
   a. Statement of Work
   b. Milestone Document
   c. Functional Specification
   d. Sign Off/Acceptance

5. Failure to meet milestone dates as agreed upon in the milestones document could present a jeopardy to the project.

6. The Client will provide SunGard Higher Education with an Acceptance Test Plan that will determine whether or not the customization meets the requirements outlined in the functional specification.

7. SunGard Higher Education will test the customization prior to delivery; however, it is the responsibility of the Client to thoroughly test the customization within the testing period allowance (30 days from the date of delivery of the customization).

8. The project will be considered accepted and complete 30 days from initial delivery, if there are no outstanding defects and a signed acceptance agreement has not been obtainable. However, a signed acceptance agreement is required before any modification is eligible for maintenance through Customization Services.

9. The Client is responsible for the installation of the software delivered by SunGard SCT.

10. The Client is responsible for data set up required by the customization.

11. End user training, beyond the delivered documentation, is not part of this estimate. General Security training will be dealt with as part of the South Dakota implementation.

12. Maintenance is not included in this Statement of Work. After original project sign off is submitted, a separate maintenance agreement is required if the Client wishes to put the customization under a maintenance contract.

13. SunGard Higher Education will perform all work off campus. On-site, campus visits are outside the scope of this estimate.

14. Travel and expenses are not included in the estimate of effort associated with this document.

15. This customization is not intended to address the security used in the functional areas related to Fund, Organization, Rule, or Approvals but instead the assignment and maintenance of user id and form/screen level security.

16. The BANSECR Oracle user would use the GSASECR form as it currently does in the baseline version. This Oracle user would only be used by the SDBOR/RIS staff for overall administration of the system needs.

17. South Dakota Board of Regents is not using Virtual Private Database technology to separate data by institution.

18. Any University Security Coordinator can alter the security of any Oracle user through the new Distributed Security form that is a part of this customization except BANSECR,
19. Naming convention of BANSECR_%XX accounts must correspond with definitions of shared classes. The details of naming conventions will be in the functional specification document.

20. Creating and maintaining classes will not initially be allowed by USC’s. Scripts will be provided that can be applied later to allow access.

1.3.3 Exclusions
This customization applies to the maintenance of user ID and form/object level security only. It does not apply to other areas within Banner that has functional security implications within individual systems, such as Fund, Organization, Rules or Approvals. It also has not impact on value based security within the baseline Banner product.

1.3.4 Concerns
Not Applicable.

1.3.5 Terminology
Not Applicable.

1.3.6 Security
This entire customization impacts the security or user id maintenance and form/object level security. The creation of distributed security BANSECR ids will have to be devised carefully as the name used impacts that login’s ability to query, insert, update and delete information.

1.3.7 Site Policy Impact
Individual security coordinators will have to work closely with the RIS staff to devise appropriate classes for security use.

1.4 Functionality

1.4.1 Functional Process Flow

The functionality that follows will describe a combination of baseline distributed security setup and the implications of the customized table policies.

1. The main BANSECR account is used by RIS staff to maintain the overall system security. This account will NOT be impacted at all by this customization.
2. Additional BANSECR_%XX accounts are created following the information documented in the SCT Banner General/Security Technical Reference Manual available through the Support Center for downloading. These accounts will be created for distributed security roles (specifically for the University Security Coordinators (USCs)). The last two characters are critical for establishing the security user’s access.

3. Per the distributed security setup, and the desired functionality for USCs, the USC BANSECR_%XX will be created without the following privileges:
   a. Alter, grant or drop any role
   b. Alter, create or drop any user
   c. Update on BANSECR.GUBIPRF
   d. Update on BANSECR.GURAOBJ

4. Per the distributed security setup, and the desired functionality for USCs, the USC BANSECR_%XX will be created with the following privileges:
   a. Update on BANSECR.GTVCLAS
   b. Update on BANSECR.GURALOG
   c. Update on BANSECR.GURUCLS
   d. Update on BANSECR.GURUOBJ

5. Security users will log in to form GSASECR to maintain security information.
   a. BANSECR user will have access to all tabs and all privileges regardless of naming conventions
   b. BANSECR_%XX users will have the following access
      i. The following tabs will provide either no access or no functionality is available under the tab: Institution Profile, Objects and Roles
      ii. Classes tab
         1. Initial functionality installed:
            a. All classes will be queryable.
            b. USCs will not be able to modify, copy or otherwise maintain any classes.
         2. Additional policy script provided but not applied until deemed necessary:
            a. All classes will be displayed.
            b. Only classes that end with SHARED or begin with the same two characters that end the BANSECR_%XX can be duplicated.
            c. Only classes that begin with the same two characters that end the BANSECR_%XX can be synchronized by the user.
            d. Only classes that begin with the same two characters that end the BANSECR_%XX can be created by the user.
            e. Only classes that begin with the same two characters that end the BANSECR_%XX can be updated or deleted through the objects button by the user.

   iii. Users tab
1. Create, Delete and Alter User will not be enabled
2. Delete User will not be enabled
3. Modify Permissions will be enabled
   a. The USCs will be able to grant objects directly to users with the following restrictions:
      i. Only objects associated with at least one class will be queryable by USCs
      ii. Objects that are associated ONLY with secured classes (i.e. classes that do not end with _SHARED or classes that do not begin with two characters that match the two ending characters of the BANSECR name) can be assigned to a user but the role granted must end with _Q. This will restrict secured objects from being granted to users for maintenance privileges but will allow query access to be granted.
      iii. Objects that are associated with unsecured classes (i.e. classes that end with _SHARED or classes that begin with two characters that match the two characters that match the ending two characters of the BANSECR name) can be assigned to a user with any attached role.
      iv. (NOTE – this means that as soon as an object is associated with a shared class it opens up that object for maintenance privileges to be assigned by USCs)
   b. Can view any classes the user is assigned to.
4. Summary Permissions will be enabled
   iv. Violations tab
      1. All security violations will be viewable but no deletes will be allowed.

NOTE:
The distributed security BANSECR accounts that are created must follow a naming convention of “BANSECR_%XX” with the value that follows the percent symbol being the two character comparison value used in the Fine Grained Access Control policy. There is a two character restriction on the length of the comparison value.

1.4.2 New Human Computer Interactions (HCI)/Forms
Not Applicable.
1.4.3 Modified Human Computer Interactions (HCI)/Forms
Not Applicable.

1.4.4 New Web Applications
Not Applicable.

1.4.5 Modified Web Applications
Not Applicable.

1.4.6 New Processes
Not Applicable.

1.4.7 Modified Processes
Not Applicable.

1.4.8 New Reports
Not Applicable.

1.4.9 Modified Reports
Not Applicable.

1.4.10 New Reporting Structures
Not Applicable.

1.4.11 Modified Reporting Structures
Not Applicable.

1.5 Database

1.5.1 New Tables
Not Applicable.
1.5.2 Modified Tables

The following tables will have a new Fine Grained Access Control policy defined for them. Each policy is specific to the table and will control the ability of specific security logins to query, insert, update and delete records on the given table.

Ultimately all the tables policies combined will give SDBOR the desired functionality for Distributed Banner Form-Object Security.

There will be three levels of access for information:

- First level is the login of BANSECR will have unrestricted access to all objects within the security module
- Second level is query access only to secured objects (i.e. objects that are associated only with a secured class) and the ability to assign only shared classes to users.
- Third level is access to view and copy classes that were created by BANSECR and end with the string _SHARED but to not be able to update or delete those classes (this level will be delivered in an additional policy script that must be run at some future time when the functionality is deemed necessary).

In the following table Q = Query, U = Update, I = Insert and D = Delete.

<table>
<thead>
<tr>
<th>Table</th>
<th>Policy to be applied</th>
<th>Functional Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBA_ROLES</td>
<td>For users BANSECR and BANSECR_%XX: no restrictions</td>
<td>The user will only be able to select authorized roles when creating classes of objects.</td>
</tr>
<tr>
<td></td>
<td>The security module already requires that the role begin with BAN or USR. No additional policies are needed on this table.</td>
<td></td>
</tr>
<tr>
<td>GTVCLAS</td>
<td>For user BANSECR: no restrictions</td>
<td>The users will be able to query any class.</td>
</tr>
<tr>
<td></td>
<td>For users BANSECR_%XX: Q any class (initially delivered policy)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For users BANSECR_%XX: (additional delivered policy to be applied if desired at a later time) QUID any class that begins with the same two characters at the end of the BANSECR login</td>
<td></td>
</tr>
<tr>
<td>GTVVPDI</td>
<td>No policy. This table is not being used by SDBOR since it applies to VPD only.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

Not applicable.
<table>
<thead>
<tr>
<th>GUBIPRF</th>
<th>QUID by BANSECR only.</th>
<th>Only the main BANSECR account will have access to this table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUBROLE</td>
<td>QUID by BANSECR only.</td>
<td>Only the main BANSECR account will have maintenance access to this table.</td>
</tr>
<tr>
<td></td>
<td>BANSECR_%XX users will have query access to all roles. The security module already restricts access only to those roles that begin with BAN or USR.</td>
<td>BANSECR_%XX users will have query access to this table.</td>
</tr>
<tr>
<td>GURALOG</td>
<td>Q by All and UID by BANSECR only.</td>
<td>All security users will be able to query the table but only BANSECR can delete the records.</td>
</tr>
<tr>
<td>GURSQLL</td>
<td>QUID by BANSECR only.</td>
<td>Only the main BANSECR account will have access to this table.</td>
</tr>
<tr>
<td>GURUCLS</td>
<td>For user BANSECR: no restrictions</td>
<td>Initial policy delivered the user will be able to query any class (secured and shared) but can only assign classes that end with _SHARED.</td>
</tr>
<tr>
<td></td>
<td>For users BANSECR_%XX: Q any assigned class, insert any assigned class that ends with _SHARED (initially delivered policy)</td>
<td>If the additional policy is applied at a later date, the user will be able to query any class (secured and shared) and could assign classes that end with _SHARED or classes that begin with the same two characters as the ending of their user name.</td>
</tr>
<tr>
<td></td>
<td>For users BANSECR_%XX: (additional delivered policy to be applied if desired at a later time) QUID any assigned class (GURUCLS_CLASS_CODE) that begins with XX where the first two characters of the class matches the last two characters of the BANSECR login</td>
<td></td>
</tr>
<tr>
<td>GURUOBJ</td>
<td>For user BANSECR no restrictions</td>
<td>Initial policy delivered the user will be able to query any object that has been associated with an individual user or class. They can also insert, update and delete new objects to a user individually if the object is associated with a</td>
</tr>
<tr>
<td></td>
<td>Initially delivered policy: For users BANSECR_%XX: This policy is more complex than any of the others:</td>
<td></td>
</tr>
</tbody>
</table>
- Q any object that already exists on the GURUOBJ table
- UID without a GURUOBJ_ROLE restriction any record where a second select on the GURUOBJ table returns a GURUOBJ_USERID that ends with _SHARED.
- UID with a GURUOBJ_ROLE restriction that the role code must end with _Q where a second select on the GURUOBJ table does not return a GURUOBJ_USERID that ends with _SHARED.

Additional delivered policy to be applied if desired at a later time

For users BANSECR_%XX:
- Q any object that already exists on the GURUOBJ table
- UID without a GURUOBJ_ROLE restriction any record where a second select on the GURUOBJ table returns a GURUOBJ_USERID that ends with _SHARED or begins with the same two characters that ends the BANSECR login name
- UID with a GURUOBJ_ROLE restriction that the role code must end with _Q where a second select on the GURUOBJ table does not return a class that ends with _SHARED and can grant either query or maintenance privileges to that object (the role). They can also insert, update and delete new objects to a user individually if the object is associated with a secured class (i.e. not _SHARED) but are restricted to granting only query access to that object.

If the additional policy is applied at a later date, the user will be able to query any object that has been associated with an individual user or class. They can also insert, update and delete new objects to a user individually if the object is associated with a class that ends with _SHARED or a class that has the same beginning two character string as their BANSECR login ID ends with and can grant either query or maintenance privileges to that object (the role). They can also insert, update and delete new objects to a user individually if the object is associated with a secured class (i.e. not _SHARED) but are restricted to granting only query access to that object.
1.5.3 New Views
Not Applicable.

1.5.4 Modified Views
Not Applicable.

1.5.5 New Functions
Not Applicable.

1.5.6 Modified Functions
Not Applicable.

1.5.7 New Procedures
Not Applicable.

1.5.8 Modified Procedures
Not Applicable.

1.5.9 New Packages
Not Applicable.
1.5.10 Modified Packages
   Not Applicable.

1.5.11 New Other
   Not Applicable.

1.5.12 Modified Other
   Not Applicable.

2 Cross Enterprise Considerations

   2.1.1 Campus Pipeline/Luminis
       Not Applicable.

   2.1.2 SunGard SCT Workflow Examples
       Not Applicable.

   2.1.3 WebCT Interface Processes
       Not Applicable.

   2.1.4 Learning Systems
       Not Applicable.

   2.1.5 Other Interfaced Systems
       Not Applicable.

3 Contract Information

<table>
<thead>
<tr>
<th>Modification Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Proposal Date:</td>
</tr>
</tbody>
</table>

Initial Proposal Date:
<table>
<thead>
<tr>
<th>Product(s) Targeted for Modification:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intended Release:</td>
</tr>
</tbody>
</table>

**Institutional Data**

| Product(s) Currently in Use: |

**Client Contact(s)**

1. Last Name: 
   First Name: 
   Telephone Number: 
   Email Address: 

2. Last Name: 
   First Name: 
   Telephone Number: 
   Email Address:
4 Approval to Proceed

The signatures below indicate that SDBOR 003 Distributed Banner Form-Object Security Specification 3.0.doc meets the approval of the undersigned and thereby grants SunGard SCT the approval to proceed.

Please fax this approval page to Melissa Shearer at 610-578-3110.

________________________________________  ______________
Signature                  Date

Print Name:  
Print Title: 

________________________________________  ______________
Signature                  Date

Print Name:  
Print Title: 

________________________________________  ______________
Signature                  Date

Print Name:  
Print Title: 
5 Document History

<table>
<thead>
<tr>
<th>Number</th>
<th>Date and Sections</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>03/20/2006</td>
<td>Melissa Shearer</td>
<td>Original Specification</td>
</tr>
<tr>
<td>2.0</td>
<td>03/29/2006</td>
<td>Melissa Shearer</td>
<td>Updated after discussion with client and confirmation of possible solutions that can be offered through internal tech resources</td>
</tr>
<tr>
<td>3.0</td>
<td>03/31/2006</td>
<td>Melissa Shearer</td>
<td>Updated the class section for the optional policy so that class naming convention has a prefix for comparison values but the BANSECR id has a suffix for comparison values. Updated the comparison value restriction to be 2 characters only (as suffix for the BANSECR id and prefix for Classes)</td>
</tr>
</tbody>
</table>
### 6 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMC</td>
<td>Account Management Council</td>
</tr>
<tr>
<td>AMM</td>
<td>Account Management Methodology</td>
</tr>
<tr>
<td>CAM</td>
<td>Client Account Management</td>
</tr>
<tr>
<td>CDM</td>
<td>Common Development Methodology</td>
</tr>
<tr>
<td>CMS</td>
<td>Common Star</td>
</tr>
<tr>
<td>CSM</td>
<td>Common Services Methodology</td>
</tr>
<tr>
<td>PEG</td>
<td>Process Engineering Group</td>
</tr>
<tr>
<td>PMC</td>
<td>Project Management Council</td>
</tr>
<tr>
<td>PMM</td>
<td>Project Management Methodology</td>
</tr>
<tr>
<td>ProNet</td>
<td>SunGard SCT’s Process Network</td>
</tr>
<tr>
<td>PTDB</td>
<td>Project Tracking Database</td>
</tr>
<tr>
<td>RPE</td>
<td>Request for Product Enhancement</td>
</tr>
<tr>
<td>SPG</td>
<td>Software Process Group</td>
</tr>
<tr>
<td>SQ&amp;P</td>
<td>Services Quality and Processes</td>
</tr>
</tbody>
</table>

### 7 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>