

PDR RID Report

Date Last Modified 3/28/95
Originator Gaylord, Arthur S. **Phone No** 413-545-2520
Organization Project Pilgrim, Univ. of Massachusetts
E Mail Address art@cs.umass.edu
Document CSMS Requirements Spec (304-CD-003-001)

RID ID	PDR	204
Review	CSMS	
Originator Ref		
Priority	2	

Section 6.3.3.2

Page 6-28

Figure Table NA

Category Name Requirements

Actionee HAIS

Sub Category

Subject Security Authorization Requirements

Description of Problem or Suggestion:

Requirement C-CSS-21110 states that "the Security Service shall authenticate the principal before checking whether the principal is authorized to access a service." This is a significant and unnecessary access restriction as ACLs can be constructed (and standardly are within DCE) to specify what access, if any, will be allowed to unauthenticated users. Also authentication of principals should not be initiated by another service.

It should be recognized that ACLs are not only associated with servers but also resources that servers interact with. For example, the permissions to access a print server, a printer that it serves, and a file to be printed can all be different. Each of these 3 "resources" can have a different ACL and each requires security checks at different times. This is not adequately reflected in requirements C-CSS-21130 - 21160

Originator's Recommendation

The role of ACLs and their manipulation in a distributed environment is critical to its operation and maintenance. This section should be reviewed and revised.

GSFC Response by:

GSFC Response Date

HAIS Response by: Forman

HAIS Schedule 2/28/95

HAIS R. E. N. Hota

HAIS Response Date 2/28/95

The requirement was not stated correctly. The intention here is to state that CSMS will provide the capability for service providers to authenticate the clients before checking their authorization privileges to access a service. The service providers don't have to use it. It is an optional capability for them to use it before checking the authorization privileges. Will restate the requirement to "The CSS Security service shall provide the capability for the service providers to authenticate principals before checking whether the principal is authorized to access a service."

It is stated in the Authorization section that "authorization is the process of deciding whether a given users/principals should be allowed to access a specified service/resource and then allow/deny the service". Will change that to "authorization is the process of deciding whether a given users/principals should be allowed to access a specified service/resource and then allow/deny access to that service/resource".

In addition, all the requirements C-CSS-21110 to C-CSS-21160 will be modified to change "server" to "resource" to reflect that the authorization is for accessing a resource.

Status **Closed**

Date Closed **3/28/95**

Sponsor **Broder**

Official RID Report

PDR RID Report

Status **Closed**

Date Closed **3/28/95**

Sponsor **Broder**

***** Attachment if any *****
