HRAC RFP Submission: Outstanding Issues

Title	**Access Control**
ID	1
Should be addressed in	Initial
Description	1. What is the model/mechanism? 2. Is the model/mechanism fixed or extensible? If extensible, how so? 3. Does the rules of the model/mechanism use resource content as security metadata?
Date Issued	8/10/98
Depends on Issues	8, 9
Pointed by	John Barkley
Related Refs	
To propose a resolution	
Resolution description	

Title	**Consistent Terminology**
ID	7
Should be addressed in	Initial
Description	Can we define some consistent Terminology?
Date Issued	8/10/98
Depends on Issues	11, 12, 13
Pointed by	Carol Burt
Related Refs	msg00039.html
To propose a resolution	
Resolution description	

Title	**Resource Security Metadata**
ID	8
Should be addressed in	Initial
Description	I can see the following 3 ways to obtain resource security metadata (I use words "metadata" and "data" to mean the same type of data unless specified otherwise): 1. Pass only resource id to the ADO. In order to obtain the data the ADO is supposed to go elsewhere and use resource id to find the data. 2. Pass only resource id to the ADO and use it as a carrier of the data. Where as, a. data syntax and semantics of the data are predefined and assumed. b. data syntax is not assumed. Data is represented by parsable tag-like structures. Semantics of data is predefined elsewhere. c. syntax and semantics of data are defined elsewhere and a reference to those definitions is passed along the data itself. Each way has pros and cons. What one (or more than one) should be used in this submission?
Date Issued	8/10/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	[hrac resources] thread in the mail list of the submitting team
To propose a resolution	
Resolution description	

Title	**Resource Identifier Structure**
ID	9
Should be addressed in	Initial
Description	What syntax and semantics should the resource identifier have?
Date Issued	8/10/98
Depends on Issues	8
Pointed by	Carol Burt
Related Refs	[hrac resources] thread in the submission team mail list + minutes from July 30 meeting of
To propose a resolution	
Resolution description	

Title	**Understanding of application functionality or data**
ID	10
Should be addressed in	Initial
Description	Should HRAC understand application data/functionality?
Date Issued	8/11/98
Depends on Issues	14
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	Bob Burt: I propose that HRAC should have no understanding of application functionality or data.

Title	**Defintion of "Resource Name"**
ID	12
Should be addressed in	Initial
Description	What is a resource name?
Date Issued	8/11/98
Depends on Issues	11
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	Bob Blakley
Resolution description	Bob Burt: I propose that it is an identifier for an application defined resource. Its format may be as simple as: type sequence<string> ResourceName;

Title	**Defintion of "Resource Metadata"**
ID	13
Should be addressed in	Initial
Description	What is resource metadata?
Date Issued	8/11/98
Depends on Issues	11
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	Bob Burt: I propose that resource metadata is data that describes a resource. Note: "describes" does not mean provides the value of the resource. I suggest that HRAC has no requirement to maintain, obtain, or use this meta data. If it exists or is used, it is strictly an application issue.

Title	**Information passed to the decision maker logic**
ID	14
Should be addressed in	Initial
Description	What information does an application pass to the decision maker logic?
Date Issued	8/11/98
Depends on Issues	No dependencies
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	Bob Burt: I propose that it pass: 1. A resource name 2. An operation name 3. A User Credential (collection of attributes(principal, group, roles)

Title	**Operation Format**
ID	15
Should be addressed in	Initial
Description	What is the format of an operation?
Date Issued	8/11/98
Depends on Issues	14
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	Bob Burt: I propose that it can be as simple as: typedef string Operation;

Title	**Authorization rule specification**
ID	16
Should be addressed in	Initial
Description	How are rules specified?
Date Issued	8/11/98
Depends on Issues	No dependencies
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	Bob Burt: I propose that each ResourceName-Operation pair has the following assoicated with it: 1. One or more credential attributes 2. A sequence of time-pairs Permission is granted if "any" of the user credential attributes match "any" of the associated credential attributes and the current time does not fall in one of the time-pairs period of time. If resources are used in a hierarchial fashion, that is, the resource name has more than one name in it's sequence, then subsetting of rules should be enforced. One might want to further define something called a policy object that would be a matrix of operations x attributes. The policy object could have a name an be used in the future without rebuilding the matrix.

Title	**Goals for Initial submission**
ID	17
Should be addressed in	Initial
Description	What else is needed for an initial submission?
Date Issued	8/11/98
Depends on Issues	10-16
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	Bob Burt: I propose as little as possible. Some examples might be: 1. Callback mechanism for rules changes. 2. Interface to defining resources/rules. 3. More complexity in Resourse Name, perhaps to indicate resource types, etc.

Title	**Contents of a resource reference**
ID	19
Should be addressed in	Initial
Description	Should the contents of a resource reference be opaque or implementation-dependant?
Date Issued	8/11/98
Depends on Issues	14, 20
Pointed by	John Barkley
Related Refs	minutes of the conference call of August 11, 1998
To propose a resolution	
Resolution description	

Title	**Definition of "Resource Reference" term**
ID	20
Should be addressed in	Initial
Description	What does term "resource reference" mean?
Date Issued	8/11/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	August 11, 1998, conference call minutes
To propose a resolution	Bob Blakley
Resolution description	

Title	**Locality constrainness of ADO**
ID	5
Should be addressed in	Revised
Description	Should an Access Decision Object to be locality constrained?
Date Issued	8/10/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	
To propose a resolution	
Resolution description	

Title	**Quality of Protection as an authorization decision factor**
ID	6
Should be addressed in	Revised
Description	Should current quality of protection policy information in ADO client be used as a factor in authorization decisions as principal credentials are?
Date Issued	8/10/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	msg00055.html -- msg00057.html
To propose a resolution	
Resolution description	

Title	**ADO interfaces Exceptions**
ID	2
Should be addressed in	Final
Description	What exceptions should be raised by ADO's methods? Should it be the matter of a policy whether ADO raises an exception when something goes wrong ot silently denies access to a resource? Three possible directions are identified: 1. Methods raise no exceptions 2. Methods raise exceptions a. Methods raise only system exceptions (like NO_PERMISSION, BAD_PARAM, NOT_IMPLEMENT) b. Methods raise system and application exceptions,
Date Issued	8/11/98
Depends on Issues	
Pointed by	Konstantin Beznosov
Related Refs	mail list archive messages # msg00040.html, msg00054.html
To propose a resolution	
Resolution description	

Title	**Exception(s) raised by multiple_action_access_allowed() method in ADO interface**
ID	4
Should be addressed in	Final
Description	From her message: "Should access decision methods throw exceptions at all... an audit log should have this info... but not the client... seems it should be a binary decision." Derived from a conference call discussion: How would a programmer use an exception returned by multiple_action_access_allowed() method? Is not it better return any problem indications in the returned sequence instead of raising an exception?
Date Issued	8/10/98
Depends on Issues	2
Pointed by	Carol Burt
Related Refs	
To propose a resolution	
Resolution description	

Title	**Correct name of the specified functionality: no "access control" but "athorization decisions"**
ID	18
Should be addressed in	Final
Description	"HRAC" stands for healthcare resource access control. Clearly, the functionality for which the RFP is asking (and what a submission is supposed to specify) is concern only with making authorization decisions, i.e. no actual access control is in the scope of the RFP. Thus, the specified functionality should be renamed from "access control" to something else that would reflect the fact that it specifies only authorization decision part, i.e. not control.
Date Issued	8/11/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	msg00110.html
To propose a resolution	
Resolution description	

Title	**Facility or Service**
ID	21
Should be addressed in	Final
Description	Should the final functionaility be called a "facility", "service", or something else?
Date Issued	8/11/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	No additional references
To propose a resolution	Nobody Assigned
Resolution description	