HRAC RFP Submission: Resolved Issues

Title	**Access Control**
ID	1
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	11/18/98 Date Resolved 10/ 7/98
Depends on Issues	8, 9
Pointed by	John Barkley
Related Refs	
To propose a resolution	
Resolution description	The initial submission text provides the object model, interfaces and description of the mechanisms

---

Title	**Resource Security Metadata**
ID	8
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 Date Resolved 10/ 7/98
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	Approach #1 was chosen by the initial submission

Title	**Resource Identifier Structure**
ID	9
Description	What syntax and semantics should the resource identifier have?
Date Issued	8/10/98 Date Resolved 10/ 7/98
Depends on Issues	8
Pointed by	Carol Burt
Related Refs	[HRAC resources] thread in the submission team mail list + minutes from July 30 meeti
To propose a resolution	
Resolution description	The submission does not have notion of resource identifiers. It manipulates only with resource names. A resource name is a sequence of strings. It does not have predefined semantics

Title	**Understanding of application functionality or data**
ID	10
Description	Should HRAC understand application data/functionality?
Date Issued	8/11/98 Date Resolved 10/ 7/98
Depends on Issues	14
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	HRAC should have no understanding of application functionality or data.

Title	**Definition of "Resource"**
ID	11
Description	What is a resource?
Date Issued	8/11/98 Date Resolved
Depends on Issues	No dependencies
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	Define "resource" exactly how it is defined in the HRAC RFP: "a 'secured resource' can be any valuable asset of an application owner, which is accessed by an application on behalf of a principal using it, and access to which is to be controlled according to the owner's interests."

Title	**Definition of "Resource Name"**
ID	12
Description	What is a resource name?
Date Issued	8/11/98 Date Resolved 10/ 7/98
Depends on Issues	11
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	Bob Burt
Resolution description	It is an identifier for an application defined resource. Its format is as follows type sequence<string> ResourceName;

Title	**Definition of "Resource Metadata"**
ID	13
Description	What is resource metadata?
Date Issued	8/11/98 Date Resolved 10/ 7/98
Depends on Issues	11
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	Bob Burt
Resolution description	Resource metadata is data that describes a resource. Note: "describes" does not mean provides the value of the resource. HRAC has no requirement to maintain, obtain, or use this meta data. If it exists or is used, it is strictly an application issue. Resource metadata is accessed/interpreted in the scope of policy evaluators, dynamic attribute evaluators, and it is out of scope of the HRAC service.

Title	**Information passed to the decision maker logic**
ID	14
Description	What information does an application pass to the decision maker logic?
Date Issued	8/11/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	Bob Burt
Resolution description	An application service (ADO client) passes: 1. A resource name 2. An operation name 3. Principal security attributes

Title	**Operation Format**
ID	15
Description	What is the format of an operation?
Date Issued	8/11/98 Date Resolved 10/ 7/98
Depends on Issues	14
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	Bob Burt
Resolution description	typedef string Operation;

Title	**Authorization rule specification**
ID	16
Description	How are rules specified? Bob Burt: I propose that each ResourceName-Operation pair has the following associated 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 hierarchical fashion, that is, the resource name has more than one name in it's sequence, then sub-setting 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.
Date Issued	8/11/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	The submission does not specify authorization rules. Instead, it provides mechanisms that allow ADO to invoke different policy evaluators that can implement various authorization models.

Title	**Goals for Initial submission**
ID	17
Description	What else is needed for an initial submission?
Date Issued	8/11/98 Date Resolved 10/ 7/98
Depends on Issues	10-16
Pointed by	Bob Burt
Related Refs	msg00108.html
To propose a resolution	
Resolution description	see the initial submission text

Title	**Contents of a resource reference**
ID	19
Description	Should the contents of a resource reference be opaque or implementation-dependant?
Date Issued	8/11/98 Date Resolved 10/ 7/98
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	No resource reference is in the submission model

Title	**Definition of "Resource Reference" term**
ID	20
Description	What does term "resource reference" mean?
Date Issued	8/11/98 Date Resolved 10/ 7/98
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	The submitted response does not use a concept "resource reference" at all.

Title	**Legacy access control engines**
ID	24
Description	There are examples of legacy access control engines which would not fit well with the interfaces proposed by Bob Blakley
Date Issued	8/25/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	Bret Hartmen and Juggy
Related Refs	msg00118.html
To propose a resolution	Bret to provide examples
Resolution description	The submission provides mechanisms to replace or add additional access control engines

Title	**Deny/grant semantics**
ID	29
Description	Where there is a resource, world is denied, group is granted, specific individual of group is denied. Cannot be handled by current interfaces.
Date Issued	9/15/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	
Related Refs	Minutes of the submitters meeting in Seattle on September 15, 1998
To propose a resolution	Nobody Assigned
Resolution description	The new (as of 10/07/98) HRAC design model does not define a particular access policy mechanism. Instead, it provided a way to have multiple access policy evaluators.

Title	**Time-dependant rights**
ID	30
Description	Do we need to capture periodic rights? For example, after hours security may be more strict
Date Issued	9/15/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	
Related Refs	Minutes of the submitters meeting in Seattle on September 15, 1998
To propose a resolution	Nobody Assigned
Resolution description	The new (as of 10/07/98) HRAC design model does not define a particular access policy mechanism. Instead, it provided a way to have multiple access policy evaluators.

Title	**Possible holes in negative states of access policies**
ID	31
Description	There are possible holes in the current access policy model as of when the issue is raised.
Date Issued	9/15/08 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	
Related Refs	Minutes of the submitters meeting in Seattle on September 15, 1998
To propose a resolution	Nobody Assigned
Resolution description	The new (as of 10/07/98) HRAC design model does not define a particular access policy mechanism. Instead, it provided a way to have multiple access policy evaluators.

Title	**Resource key and POA-based call-backs**
ID	32
Description	In application services using POA, an object key can be used by the servant manager to incarnate an appropriate servant or even to have one servant for all call-back object. In this case we do not need resource key when calling dynamic attribute service
Date Issued	9/15/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	Minutes of the submitters meeting in Seattle on September 15, 1998
To propose a resolution	Konstantin Beznosov
Resolution description	The issue was raised because of the assumption that the resource key would be used only when ADO calls back the application service that invoked the ADO. The assumption was not correct.

Title	**Locality constrainness of ADO**
ID	5
Description	Should an Access Decision Object to be locality constrained?
Date Issued	8/10/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	
To propose a resolution	
Resolution description	No, it should not. Only security attributes are passed through methods of the ADO interface. So, it's safe to have ADO ¬ locality constrained.

Title	**Required rights expression**
ID	22
Description	Taking into account that the authorization rule language in HRAC is expected, at list by me, to be more rich in its expressiveness than the one provided by CORBA security access model, I contend that just simple expression of required rights (such as "A or B or C or D" or "A and B and C and D") would not suffice. I believe that more complex expressions should be allowed.
Date Issued	9/11/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	Konstantin Beznosov
Related Refs	No additional references
To propose a resolution	Nobody Assigned
Resolution description	Any type of policy evaluator can be used within HRAC service. The required-rights model is not used by the mandatory part of the submission any more.

Title	**Typedefs in the interface modules**
ID	28
Description	When interfaces in IDL compiled into Java classes and interfaces, "typedef" statements generate dummy classes that are very inefficient to use comparatively to original types. Is there a way to avoid/solve this problem in the submitted interfaces of the spec?
Date Issued	9/15/98 Date Resolved 10/ 7/98
Depends on Issues	No dependencies
Pointed by	Bart de Greef
Related Refs	Minutes of the submitters meeting in Seattle on September 15, 1998
To propose a resolution	Nobody Assigned
Resolution description	The submission team decided that this problem belongs to the scope of IDL-> Java mapping and if it is a serious issue for developers/designers, it should be addressed through IDL->Java mapping RTF or via a new RFP in the OMG. The submission team decided to use typedef mechanisms as appropriate.

Title	**Inference of sensetive information via accessing particular non-sensetive resources**
ID	38
Description	What if a client would access 3 different resources associtated with information of low sensetivity level and then use the obtained information to infere information of higher level of sensetivity?
Date Issued	11/10/98 Date Resolved 11/10/98
Depends on Issues	No dependencies
Pointed by	Jarom Soeller
Related Refs	No additional references
To propose a resolution	Bob Blakley
Resolution description	The RFP did not ask to address this kind of issue