Object Management Group

Framingham Corporate Center
492 Old Connecticut Path
Framingham, MA 01701-4568

Telephone: +1-508-820 4300
Facsimile: +1-508-820 4303

Healthcare Resource Access Control Request For Proposal

OMG Document: corbamed/98-02-23

Submissions due: August 24, 1998

Objective of this RFP

The complexity of the healthcare security problem domain requires exercising more sophisticated access control policies rather than the general ones used in the CORBA Security service. This complexity leads system developers to proprietary solutions on top of security provided by ORB systems. At the same time, commonality of business domain tasks and security requirements across healthcare computing environments promotes and requires exercising fine-grained access control policies in a uniform and standard way. It is expected that a number of RFPs will need to be issued to fully address the security concerns and requirements of healthcare industry, including ones related to access control, auditing, nonrepudiation, and notification of security breaches, and other related themes.

This RFP solicits proposals for resource access control facilities based on the CORBA Security service. Such a facility will provide a uniform way for application systems to enforce resource-oriented access control policies in the healthcare domain.

For further details see Chapter 6 of this document.

1.0 Introduction

1.1 Goals of OMG

The Object Management Group (OMG) is the world's largest software consortium with a membership of over 800 vendors, developers, and end users. Established in 1989, its mission is to promote the theory and practice of Object Technology (OT) for the development of distributed computing systems.

A key goal of OMG is create a standardized object-oriented architectural framework for distributed applications based on specifications that enable and support distributed objects. Objectives include the *reusability*, *portability*, and *interoperability* of object-oriented software components in heterogeneous environments.To this end, the OMG adopts interface and protocol specifications, based on commercially available object technology, that together define an Object Management Architecture (OMA).

1.2 Organization of this document

The remainder of this document is organized as follows:

Chapter 2 - *Architectural Context* - background information on OMG's Object Management Architecture.

Chapter 3 - *Adoption Process* - background information on the OMG specification adoption process.

Chapter 4 - *Instructions for Submitters* - explanation of how to make a submission to this RFP.

Chapter 5 - *General Requirements on Proposals* - requirements and evaluation criteria that apply to all proposals submitted to OMG.

Chapter 6 - *Specific Requirements on Proposals* - problem statement, scope of proposals sought, mandatory and optional requirements, issues to be discussed, evaluation criteria, and timetable that apply specifically to this RFP.

Additional RFP-specific chapters may also be included following Chapter 6.

1.3 References

The following documents are referenced in this document:

Richard Soley (ed.), *Object Management Architecture Guide*, Third Edition, Wiley, June 1995. OMG Document ab/97-05-05, or successor.

The Common Object Request Broker: Architecture and Specification, Revision 2.1, August 1997. OMG Document formal/97-09-01, or successor.

CORBAservices: Common Object Services Specification, Revised Edition, July 1997. OMG Document formal/97-07-04, or successor.

CORBAfacilities Architecture, Revision 4.0, November 1995.

Business Committee RFP Attachment, OMG Document omg/97-10-01.

Policies and Procedures of the OMG Technical Process, OMG Document pp/97-06-01 or successor.

These documents can be obtained by contacting OMG at document@omg.org. Many OMG documents, including this document, are available electronically from OMG's document server. Send a message containing the single line "help" to server@omg.org for more information, or visit the OMG Web page (URL http://www.omg.org/), which also has more information about OMG in general. If you have general questions about this RFP send email to responses@omg.org.

2.0 Architectural Context

2.1 Object Management Architecture

The *Object Management Architecture Guide* (OMAG) describes OMG's technical objectives and terminology and provides the conceptual infrastructure upon which supporting specifications are based. The guide includes the *OMG Object Model,* which defines common semantics for specifying the externally visible characteristics of objects in a standard implementation-independent way, and the *OMA Reference Model.*

The Reference Model identifies and characterizes the components, interfaces, and protocols that compose the OMA. This includes the Object Request Broker (ORB) component that enables clients and objects to communicate in a distributed environment, and four categories of object interfaces:

- *Object Services* are interfaces for general services that are likely to be used in any program based on distributed objects.
- *Common Facilities* are interfaces for horizontal end-user-oriented facilities applicable to most application domains.
- *Domain Interfaces* are application domain-specific interfaces.
- *Application Interfaces* are non-standardized application-specific interfaces.

A second part of the Reference Model introduces the notion of domain-specific *Object Frameworks*. An Object Framework component is a collection of cooperating objects that provide an integrated solution within an application or technology domain and which is intended for customisation by the developer or user.

Through a series of RFPs, OMG is populating the OMA with detailed specifications for each component and interface category in the Reference Model. Adopted specifications include the Common Object Request Broker Architecture (CORBA), CORBAservices, and CORBAfacilities.

The wide-scale industry adoption of OMG's OMA provides application developers and users with the means to build interoperable software systems distributed across all major hardware, operating system, and programming language environments.

2.2 CORBA

The *Common Object Request Broker Architecture* defines the programming interfaces to the OMA ORB component. An ORB is the basic mechanism by which objects transparently make requests to - and receive responses from - each other on the same machine or across a network. A client need not be aware of the mechanisms used to communicate with or activate an object, how the object is implemented, nor where the object is located. The ORB thus forms the foundation for building applications constructed from distributed objects and for interoperability between applications in both homogeneous and heterogeneous environments.

The *OMG Interface Definition Language* (IDL) provides a standardized way to define the interfaces to CORBA objects. The IDL definition is the contract between the implementor of an object and the client. IDL is a strongly typed declarative language that is programming language-independent. Language mappings enable objects to be implemented and sent requests in the developer's programming language of choice in a style that is natural to that language.

CORBA 2.0 is an extension and restructuring of the earlier CORBA 1.2 specification. CORBA 2.0 is a family of specifications consisting of the following components:

- Core (including IDL syntax and semantics)
- Interoperability
- An expanding set of language mappings, including:

  C
  C++
  SmallTalk
  Ada95
  COBOL

Each component is a separate compliance point. The minimum required for a CORBA-compliant implementation is adherence to the core and one language mapping.

2.3 CORBA/Interoperability

Interoperability between CORBA-compliant ORBs is provided by OMG's *Internet Inter-ORB Protocol* (IIOP). Adopted in December 1994 as the mandatory CORBA 2.0 protocol for “out of the box” interoperability, IIOP is the TCP/IP transport mapping of a *General Inter-ORB Protocol* (GIOP).

IIOP enables requests to be sent to networked objects managed by other ORBs in other domains.

The OMG interoperability architecture also accommodates communication using optional *Environment-Specific IOPs* (ESIOPs), the first of which is the DCE-CIOP.

2.4 CORBAservices

Object Services are general purpose services that are either fundamental for developing useful CORBA-based applications composed of distributed objects, or that provide a universal - application domain-independent - basis for application interoperability.

Object Services are the basic building blocks for distributed object applications. Compliant objects can be combined in many different ways and put to many different uses in applications. They can be used to construct higher level facilities and object frameworks that can interoperate across multiple platform environments.

Adopted OMG Object Services are collectively called CORBAservices and include Naming, Events, LifeCycle, Persistent Object, Relationships, Externalization, Transactions, Concurrency Control, Licensing, Query, Properties, Security, Time, Collections, and Trading Services.

2.5 CORBAfacilities

Common Facilities are interfaces for horizontal end-user-oriented facilities applicable to most domains. Adopted OMG Common Facilities are collectively called CORBAfacilities and include an OpenDoc-based Distributed Document Component Facility.

A specification of a Common Facility or Object Service typically includes the set of interface definitions - expressed in OMG IDL - that objects in various roles must support in order to *provide*, *use,* or *participate in* the facility or service. As with all specifications adopted by OMG, facilities and services are defined in terms of interfaces and their semantics, and not a particular implementation.

2.6 Object Frameworks and Domain Interfaces

Unlike the interfaces to individual parts of the OMA “plumbing” infrastructure, Object Frameworks are complete higher level components that provide functionality of direct interest to end-users in particular application or technology domains. They are vertical slices down the

OMG “interface stack”.

Object Frameworks are collections of cooperating objects categorized into *Application, Domain, Facility,* and *Service Objects*. Each object in a framework supports (through interface inheritance) or makes use of (via client requests) some combination of Application, Domain, CORBAfacilities, and CORBAservices *interfaces*.

A specification of an Object Framework defines such things as the structure, interfaces, types, operation sequencing, and qualities of service of the objects that make up the framework. This includes requirements on implementations in order to guarantee application portability and interoperability across different platforms.

Domain Task Force RFPs are likely to focus on Object Framework specifications that include new Domain Interfaces for application domains such as Finance, Healthcare, Manufacturing, Telecom, Electronic Commerce, and Transportation.

3.0 Adoption Process

3.1 Introduction

OMG adopts specifications for interfaces and protocols by explicit vote on a technology-by-technology basis. The specifications selected each fill in a portion of the OMA Reference Model. OMG bases its decisions on both business and technical considerations. Once a specification is adopted by OMG, it is made available for use by both OMG members and non-members.

For more detailed information on the adoption process see the *Policies and Procedures of the OMG Technical Process*.

3.2 Rôle of Board of Directors

The OMG Board of Directors votes to formally adopt specifications on behalf of OMG. The OMG Technology Committees (Domain and Platform TCs) and Architecture Board (AB) provide technical guidance to the Board of Directors. In addition, the Business Committee of the Board provides guidance to ensure that implementations of adopted specifications are made commercially available.

3.3 Rôle of Technology Committees and Architecture Board

Submissions to RFPs are evaluated by the TC Task Force (TF) that initiated the RFP. Selected specifications are recommended to the parent TC after being reviewed by the Architecture Board for consistency with the OMA. The full TC then votes to *recommend adoption* to the OMG Board.

3.4 Role of Task Forces

The role of the initiating TF is to technically evaluate submissions and select one or more specifications that satisfy the requirements of the RFP. The process typically takes the following form:

- Voter Registration

  Interested TF members may register to participate in specification selection votes for an RFP. Registration ends on a specified date 6 or more weeks after the announcement of the registration period. The registration closure date is typically around the time of initial submissions. Companies who have submitted an LOI are automatically registered to vote.

- Initial Submissions

  Initial submissions are due by a specified deadline. Submitters normally present their proposals at the next following meeting of the TF. Initial submissions are expected to be full and complete proposals and working implementations of the proposed specifications are expected to exist at the time of submission.

- Evaluation Phase

  A period of approximately 120 days follows during which the TF evaluates the submissions. During this time submitting companies have the opportunity to revise and/or merge their initial submissions, if they so choose.

- Revised Submissions

  Final revised submissions are due by a specified deadline. Submitters again normally present their proposals at the next following meeting of the TF. Finalists may be requested to demonstrate implementations of their proposal.

- Selection Vote

  When the registered voters of the TF believe that they sufficiently understand the relative merits of the revised submissions, a specification selection vote is taken.

3.5 Goals of the evaluation

The primary goals of the TF evaluation process are to:

- Provide a fair and open process
- Force a critical review of the submissions and discussion by all members of the TF
- Give feedback to allow submitters to address concerns in their revised submissions
- Build consensus on acceptable solutions
- Enable voting members to make an informed selection decision

Submitters are expected actively to contribute to the evaluation process.

4.0 Instructions for Submitters

4.1 OMG Membership

Submissions to this RFP may only be made by Contributing or Domain Contributing members of the OMG. To submit to an RFP issued by the Platform Technology Committee an organisation must be a Contributing member at the date of the submission deadline, while for Domain Technology RFPs the submitter or submitters must be either Contributing or Domain Contributing members. Submitters sometimes choose to name other organisations that support a submission in some way; however, this has no formal status within the OMG process, and for OMG's purposes confers neither duties nor privileges on the organisations concerned.

4.2 Submission Effort

Unlike a submission to an OMG Request For Information (RFI), an RFP submission may require significant effort in terms of document preparation, presentations to the initiating TF, and participation in the TF evaluation process. Several staff months of effort might be necessary. OMG is unable to reimburse submitters for any costs in conjunction with their submissions to this RFP.

4.3 Letter of Intent

A Letter of Intent (LOI) must be submitted to the OMG Business Committee signed by an officer of your organization signifying your intent to respond to the RFP and confirming your organization's willingness to comply with OMG's terms and conditions, and commercial availability requirements. These terms, conditions, and requirements are defined in the *Business Committee RFP Attachment* and are reproduced verbatim in section 4.4 below.

The LOI should designate a single contact point within your organization for receipt of all subsequent information regarding this RFP and your submission. The name of this contact will be made available to all OMG members. The LOI is typically due 60 days before the deadline for initial submissions. LOIs must be sent by fax or paper mail to the "RFP Submissions Desk" at the main OMG address shown on the first page of this RFP.

Here is a suggested template for the Letter of Intent:

This letter confirms the intent of <___organisation required___> (the organisation) to submit a response to the OMG <___RFP name required___> RFP. We will grant OMG and its members the right to copy our response for review purposes as specified in section 4.7 of the RFP. Should our response be adopted by OMG we will comply with the OMG Business Committee terms set out in section 4.4 of the RFP and in document omg/97-10-01.

<____contact name and details required____> will be responsible for liaison with OMG regarding this RFP response.

The signatory below is an officer of the organisation and has the approval and authority to make this commitment on behalf of the organisation.

<___signature required____>

4.4 Business Committee RFP Attachment

This section contains the text of the Business Committee RFP attachment concerning commercial availability requirements placed on submissions. This attachment, available separately as document omg/97-10-01, was approved by the OMG Board in September 1997.

Commercial considerations in OMG technology adoption

A1 Introduction

OMG wishes to encourage rapid commercial adoption of the specifications it publishes. To this end, there must be neither technical, legal nor commercial obstacles to their implementation. Freedom from the first is largely judged through technical review by the relevant OMG Technology Committee; the second two are the responsibility of the OMG Business Committee. The BC also looks for evidence of a commitment by a submitter to the commercial success of products based on the submission.

A2 Business Committee evaluation criteria

A2.1 Viable to implement across platforms

While it is understood that final candidate OMG submissions often combine technologies before they have all been implemented in one system, the Business Committee nevertheless wishes to see evidence that each major feature has been implemented, preferably more than once, and by separate organisations. Pre-product implementations are acceptable. Since use of OMG specifications

should not be dependant on any one platform, cross-platform availability and interoperability of implementations should be also be demonstrated.

A2.2 Commercial availability

In addition to demonstrating the existence of implementations of the specification, the submitter must also show that products based on the specification are commercially available, or will be within 12 months of the date when the specification was recommended for adoption by the appropriate Task Force. Proof of intent to ship product within 12 months might include:

- *A public product announcement with a shipping date within the time limit.*
- *Demonstration of a prototype implementation and accompanying draft user documentation.*

Alternatively, and at the Business Committee's discretion, submissions may be adopted where the submitter is not a commercial software provider, and therefore will not make implementations commercially available. However, in this case the BC will require concrete evidence of two or more independent implementations of the specification being used by end-user organisations as part of their businesses.

Regardless of which requirement is in use, the submitter must inform the OMG of completion of the implementations when commercially available.

A2.3 Unencumbered technology

The submitter must certify that it is not aware of any claim that the specification infringes any patent, copyright, or other intellectual property right (collectively referred to in this policy statement as "IPR"). Except for this certification, the submitter will not be required to make any other warranty, and specifications will be offered by OMG for implementation "as is". If the submitter owns IPR to which an implementation of a specification based upon its submission would necessarily be subject, it must certify to the BC that it will make a suitable license available to any implementer to permit development and commercialisation of an implementation without violation of such IPR.

The submitter shall also certify that this license will be made available on commercially reasonable, non-discriminatory terms. The submitter is responsible for disclosing in detail all known restrictions and fees, placed either by the submitter or others, on technology necessary for implementation of the specification.

A2.4 Publication of the specification

Should the submission be adopted, the submitter must grant OMG (and its sublicensees) a world-wide, royalty-free licence to edit, store, duplicate and distribute both the specification and works derived from it (such as revisions and teaching materials). This requirement applies only to the written specification, not to any implementation of it.

A2.5 Continuing support

The submitter must show a commitment to continue supporting the technology underlying the specification after OMG adoption, for instance by showing the BC development plans for future revisions, enhancement or maintenance.

4.5 Responding to RFP items

4.5.1 Separate proposals

Unless otherwise indicated in Chapter 6, independent proposals are solicited for each separate item in the RFP. Each item is considered a separate architectural entity for which a proposal may be made. A submitter may respond to any or all items. Each item will be evaluated independently by the initiating TF. Submissions that do not present clearly separable proposals for multiple items may therefore be at a disadvantage.

It should be noted that a given technology (e.g. software product) may support two or more RFP items. So long as the interfaces for each item are separable, this is not precluded.

4.5.2 Complete proposals

Proposals for each separate RFP item must be complete. A submission must propose full specifications for each item and address all the relevant general and specific requirements detailed in this RFP.

4.5.3 Additional specifications

Submissions may include additional specifications for items not covered by the RFP which they believe to be necessary and integral to their proposal. Information on these additional items should be clearly distinguished.

Submitters must give a detailed rationale as to why these specifications

should also be considered for adoption. However submitters should note that a TF is unlikely to consider additional items that are already on the roadmap of an OMG TF, since this would pre-empt the normal adoption process.

4.5.4 Alternative approaches

Submitters may provide alternative RFP item definitions, categorizations, and groupings so long as the rationale for doing so is clearly stated. Equally, submitters may provide alternative models for how items are provided within the OMA if there are compelling technological reasons for a different approach.

4.6 Confidential and Proprietary Information

The OMG specification adoption process is an open process. Responses to this RFP become public documents of the OMG and are available to members and non-members alike for perusal. No confidentiality or proprietary information of any kind will be accepted in a submission to this RFP.

4.7 Copyright Waiver

If a submitted document is copyrighted, a waiver of copyright for unlimited duplication by the OMG is required to be stated in the document. In addition, a limited waiver of copyright is required that allows each OMG member to make up to fifty (50) copies of the document for review purposes only.

4.8 Proof of Concept

Submissions must include a “proof of concept” statement, explaining how the submitted specifications have been demonstrated to be technically viable. The technical viability has to do with the state of development and maturity of the technology on which a submission is based. This is not the same as commercial availability. Proof of concept statements can contain any information deemed relevant by the submitter, for example:

> “This specification has completed the design phase and is the process of being prototyped.”
>
> “An implementation of this specification has been in beta-test for 4 months.”
>
> “A named product (with a specified customer base) is a realization of this specification.”

It is incumbent upon submitters to demonstrate to the satisfaction of the TF the technical viability of their proposal. OMG will favour proposals based on technology for which sufficient relevant experience has been gained in CORBA-based or comparable environments.

4.9 Format of RFP Submissions

This section provides guidance on how to structure your RFP submission.

4.9.1 General

- Submissions that are concise and easy to read will inevitably receive more consideration.
- Submitted documentation should be confined to that directly relevant to the items requested in the RFP. If this is not practical, submitters must make clear what portion of the documentation pertains directly to the RFP and what portion does not.
- The models and terminology in the *Object Management Architecture Guide* and *CORBA* should be used in your submission. Where you believe this is not appropriate, describe and provide a rationale for the models and terminology you believe OMG should use.

4.9.2 Suggested Outline

A three part structure for submissions is suggested:

PART I

- Copyright Waiver (see 4.5)
- Submission contact point (see 4.2)
- Overview or guide to the material in the submission
- Overall design rationale (if appropriate)
- Statement of proof of concept (see 4.6)
- Resolution of RFP mandatory and optional requirements

  Explain how your proposal satisfies the mandatory and (if applicable) optional requirements stated in Chapter 6. References to supporting material in Part II should be given.

In addition, if your proposal does not satisfy any of the general requirements stated in Chapter 5, provide a detailed rationale.

- Responses to RFP issues to be discussed

  Discuss each of the "Issues To Be Discussed" identified in Chapter 6.

PART II

- Proposed specification

PART III

- Summary of optional versus mandatory interfaces

  Submissions must clearly distinguish interfaces that all implementations must support from those that may be optionally supported.

- Proposed compliance points

  Submissions should propose appropriate compliance points for implementations.

- Changes or extensions required to adopted OMG specifications

  Submissions must include a full specification of any changes or extensions required to existing OMG specifications. This should be in a form that enables "mechanical" section-by-section revision of the existing specification.

- Complete IDL definitions

  For reference purposes and to facilitate electronic usage, submissions should reproduce in one place a complete listing in compilable form of the IDL definitions proposed for standardization.

4.10 How to Submit

Submitters should send an electronic version of their submission to the *RFP Submissions Desk* (rfp@omg.org) at OMG by 5:00 PM U.S. Eastern Standard Time (22:00 GMT) on the day of the submission deadline. Acceptable formats are Postscript, ASCII, PDF, FrameMaker, Word, and WordPerfect. However, it should be noted that a successful submission must be supplied to OMG's technical editors in Framemaker source format, using the most recent available OMG submission template (document ab/96-06-02 at the time of writing). The AB will not endorse adoption of any submission for which appropriately-formatted

Framemaker sources are not available; it may therefore be convenient to prepare all stages of a submission using this template.

Submitters should make sure they receive electronic or voice confirmation of the successful receipt of their submission. Submitters should also send, within three (3) working days after the submission deadline, a single hardcopy version of their submission to the attention of the “RFP Submissions Desk” at the main OMG address shown on the first page of this RFP.

In addition, submitters are responsible for making available 100 paper copies to attendees of the TF meeting immediately following a submission deadline. There are normally two such presentation meetings, one for the initial and one for the revised submissions.

5.0 General Requirements on Proposals

5.1 Mandatory Requirements

5.1.1 Proposals shall express interfaces in OMG IDL. Proposals should follow accepted OMG IDL and CORBA programming style. The correctness of the IDL shall be verified using at least one IDL compiler (and preferably more then one). In addition to IDL quoted in the text of the submission, all the IDL associated with the proposal shall be supplied to OMG in compiler-readable form.

5.1.2 Proposals shall specify operation behaviour, sequencing*, and* side-effects *(if any).*

5.1.3 Proposals shall be precise *and* functionally complete*. There should be no implied or hidden interfaces, operations, or functions required to enable an implementation of the proposed specification.*

5.1.4 Proposals shall clearly distinguish mandatory *interfaces and other specification elements that all implementations must support from those that may be* optionally *supported.*

5.1.5 Proposals shall reuse *existing OMG specifications including CORBA, CORBAservices, and CORBAfacilities in preference to defining new interfaces to perform similar functions.*

5.1.6 Proposals shall justify and fully specify any changes or extensions *required to existing OMG specifications. This includes changes and extensions to CORBA inter-ORB protocols necessary to support interoperability. In general, OMG favours* upwards compatible *proposals that minimize changes and extensions to existing OMG specifications.*

5.1.7 Proposals shall factor out functions that could be used in different contexts and specify their interfaces separately. Such minimality *fosters re-use and avoids functional duplication.*

5.1.8 Proposals shall use or depend on other interface specifications only where it is actually necessary. While re-use of existing interfaces to avoid duplication will be encouraged, proposals should avoid gratuitous use.

5.1.9 Proposals shall specify interfaces that are compatible *and can be used with existing OMG specifications. Separate functions doing separate jobs should be capable of being used together where it makes sense for them to do so.*

5.1.10 Proposals shall preserve maximum implementation flexibility.

Implementation descriptions should not be included, however proposals may specify constraints on object behaviour that implementations need to take into account over and above those defined by the interface semantics.

5.1.11 *Proposals shall allow* independent implementations *that are* substitutable *and* interoperable*. An implementation should be replaceable by an alternative implementation without requiring changes to any client.*

5.1.12 *Proposals shall be compatible with the architecture for system distribution defined in ISO/IEC 10746, Reference Model of Open Distributed Processing (ODP). Where such compatibility is not achieved, the response to the RFP must include reasons why compatibility is not appropriate and an outline of any plans to achieve such compatibility in the future.*

5.1.13 *In order to demonstrate that the service or facility proposed in response to this RFP, can be made secure in environments requiring security, answers to the following questions shall be provided:*

- What, if any, are the security sensitive objects that are introduced by the proposal?
- Which accesses to security-sensitive objects must be subject to security policy control?
- Does the proposed service or facility need to be security aware?
- What CORBAsecurity level and options are required to protect an implementation of the proposal? In answer to this question, a reasonably complete description of how the facilities provided by the level and options (e.g. authentication, audit, authorization, message protection etc.) are used to protect access to the sensitive objects introduced by the proposal shall be provided.
- What default policies should be applied to the security sensitive objects introduced by the proposal?
- Of what security considerations must the implementers of your proposal be aware?

5.2 Evaluation criteria

Although the OMG adopts interface specifications, the technical viability of implementations will be taken into account during the evaluation process. The following criteria will be used:

5.2.1 Performance

Potential implementation trade-offs for performance will be considered.

5.2.2 Portability

The ease of implementation on a variety of ORB systems and software platforms will be considered.

5.2.3 Securability

The answer to questions in section 5.1.13 shall be taken into consideration to ascertain that an implementation of the proposal is securable in an environment requiring security.

5.2.4 Compliance: Inspectability and Testability

The adequacy of proposed specifications for the purposes of compliance inspection and testing will be considered. Specifications should provide sufficient constraints on interfaces and implementation characteristics to ensure that compliance can be unambiguously assessed through both manual inspection and automated testing.

6.0 Specific Requirements on Proposals

Meaning of words shown in *italics* (except reserved words *may* and *shall*) is defined in section 6.9.1.

6.1 Problem Statement

There is a need to support two groups of access control policies to handle the requirements and needs of the various groups involved in the healthcare process. These are:

1) Access policies that are general and are geared to the nature of care, role of care provider and rationale for a particular disclosure or access to patient confidential information. These types of access policies are patient non-specific.

2) Access policies, which are based on the needs and requirements of a specific patient. These access policies may be based, in addition, on the actual information being accessed or disclosed.

Also, there is need in a process for handling exceptions to the rules established by such policies. Whatever such policies are, as an information system vendor, one needs to provide the mechanisms to implement such policies. For further background information on various groups and types of security policies in healthcare, several references are provided in section 6.4.

Deciding what information about a patient can or need to be disclosed depends on various factors such as role of the person seeking information, the goals and policies of the organization having the information and the legal and other rights of the patient about whom the information is sought.

Below are examples of some access control problems in healthcare. Each example consists of a policy statement, an IDL interface operation, and a rule. The policy is a high level description of a security objective. The rule is an interpretation of the policy with respect to the IDL interface operation.

1. Policy: Care providers in the emergency department are allowed to read preliminary radiology reports.

   Report retrieve_report(in PersonID pid, in Date date);

Rule: The operation is allowed if the return value is a secured resource in category *PreliminaryRadiologyReport* and the requesting principal's role attribute is *EmergencyCareProvider*.

2. Policy: A responsible party can "sign-off" on a document.

   Sign_off (in Document document);

   Rule: This operation is allowed if *document.responsible_parties* contains the access identity attribute of the requesting principal.

3. Policy: Only a registration clerk can access patient home address or social security number.

   ```
   Profile get_profile(
           in PersonID id,
           in SpecifiedTraits traits_requested
       );
   ```

   Rule: This operation is allowed if the requesting principal's role attribute is *registration_clerk* and *traits_requested* is *home_addr* or *ssnumber*.

4. Policy: All patients can read their own identity information (below we show a PIDS example)

   Identity get_identity_object (in Person_id)

   Rule: This operation is allowed if the *access identity* attribute of the requesting principal refers to the same person as *Person_id*.

5. Policy: Peer review committee members can access patient record information for all patients.

   Report retrieve_report(in PersonID pid, in Date date);

   Rule: This operation is allowed if the *role* attribute of the requesting principal is *peer_reviewer*.

The purpose of this RFP is to squarely address the ***mechanisms*** to support such sophisticated access control.

As someone can realize, similar requirements on sophisticated access control exist in some other vertical domains such as finance, electronic commerce, etc. While it is expected that submissions to this RFP can be applicable to other domains, the requirements of this RFP are drawn from the healthcare domain.

CORBAservices, including the CORBA Security Service, and CORBAfacilities provide a general-purpose infrastructure for developing distributed object systems in a broad range of specialized vertical domains. The CORBA Security service defines the interfaces to a collection of objects that provide a versatile set of services for enforcing a range of security policies using diverse security mechanisms. Some of these mechanisms require application systems to be aware of security. Upcoming CORBAmed specifications and experience from the first medical application systems based on CORBA technology reveal the necessity of sophisticated security models in medical systems. Such security models currently require application system vendors to implement complex security policies based on *content* and *context* of client➔target object interactions.

Mechanisms to express such security policies can include but are not limited to the following information taken into account:

1) Type of access operation

2) Principal id

3) Principal role

4) Principal group membership

5) Relationship between a patient and a caregiver

6) Method input argument values

7) Return result values (returned data content)

8) Time of service request

9) Location of service requester

CORBA Security service provides access control based on interface method and items 2 through 4 from the list above. Also, Principal Privilege Attributes are available for a security aware application from

CORBA Security service. They provide such information as principal access id, group membership, role, and some other.

The practical effect of not being able to use the CORBA Security Service to express or realize healthcare security policies is that each application must contain its own implementation of object instance security services. This poses severe problems for enterprises that then attempt to integrate several such applications and find that, although the functional aspects of the applications can be integrated using a CORBA infrastructure, different security models and mechanisms prevent the integrated management of the applications' security. This leaves healthcare and other enterprises with an excessive security management burden that often results in the misuse or elimination of important security measures.

This RFP seeks to provide access control mechanisms based on CORBA Services and CORBA Facilities, specifically on the CORBA Security service, that will allow enforcing resource-oriented access control in an exchangeable fashion across healthcare and other enterprises.

6.2 Scope of Proposals Sought

Mechanisms this RFP is asking for are sought to allow application systems to be unaware of advanced security policies existing in healthcare enterprises where those systems are deployed.

This RFP scope is threefold:

1. to de-couple access control decision logic from application logic,

2. to provide a standard interface for the definition of access control rules,

3. to provide a standard interface for requesting access control decisions.

An illustration of the RFP scope is provided in Figure 1. The RFP scope is limited to the additional security decision logic shown in the figure with striped background. It has a "Decision" interface to an interceptor(s) performing access control functions and an application itself to consult such Security Decision Logic for access control decisions. The "Admin" interface allows defining access control rules.

Target object implementations have business logic implemented in them. Where as, the logic responsible for making various security policy

decisions is de-coupled from the object implementation. As the picture shows, additional access control can be enforced on the level of interceptors. Such an interceptor consults the “Access Control Decision Logic” via the same “Decision” interface as a target object implementation does.

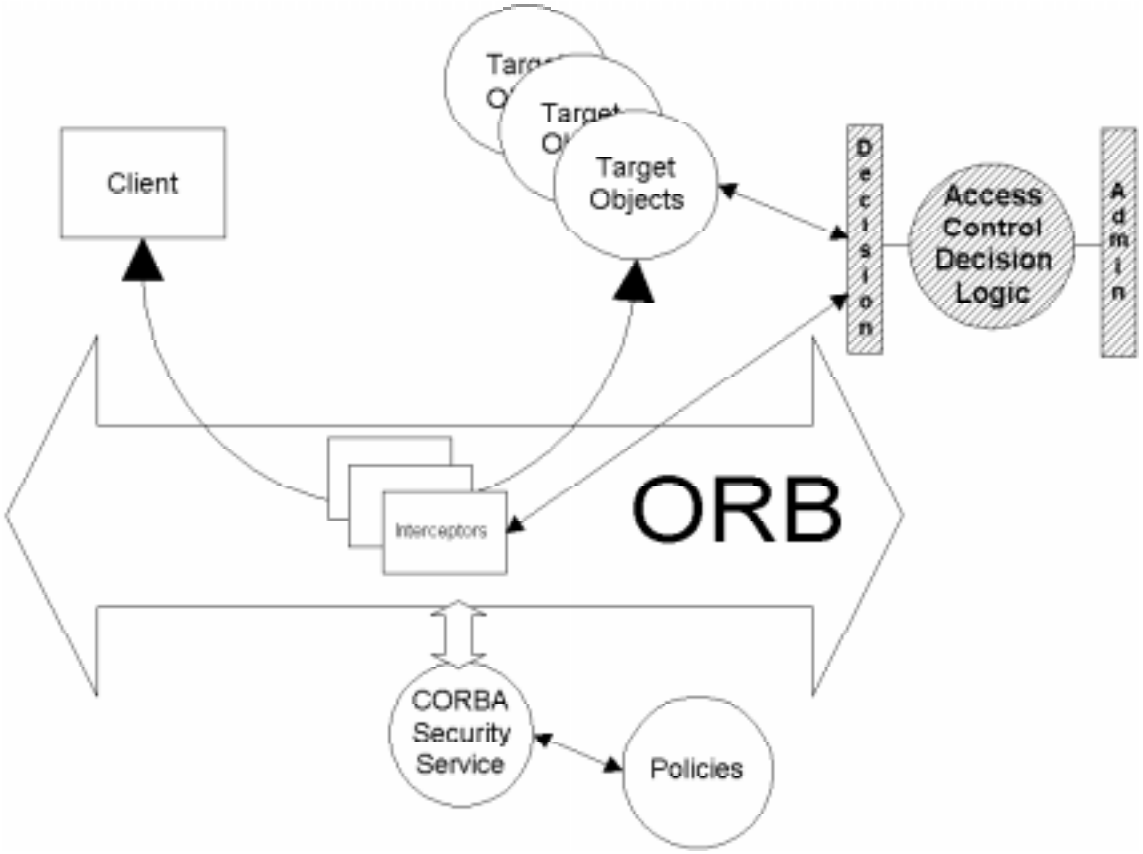

Figure 1: A Possible Solution

Since the “Decision” interface is specified, a healthcare (and other domain) vendor can implement its application services (“target objects” in the figure) without having to deal with any particular access control policies enforced in a given healthcare enterprise. Responsibilities of a target object are limited only to:

1. “Consulting” with “Security Decision Logic” via “Decision” interface provided to it.

2. Performing actions according to decisions “received” from the “Security Decision Logic”, such as denying or granting access

A healthcare enterprise administrator enforces some security policies via corresponding interfaces of CORBA Security Service. Other additional

access control policies, which take into account information discussed in the RFP, are administrated and enforced via “Access Control Decision Logic.”

This RFP asks for a solution that will utilize notion of “secured resources” instead of the notion of client←→target object interaction content. The latter is too intimate to the application logic itself. Access to “secured resources” is considered to be the essence of the most client←→target object interactions.

In the scope of this 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. For example, electronic patient medical records in a hospital are usually its valuable assets. The hospital is interested in controlling access to the records due to various legal, financial and other reasons. Therefore, the hospital considers such records as “secured resources.” Moreover, different information in those records count as different “secured resources.” Depending on privilege attributes a principal has and depending on secured resources as well as on access operation to be performed on such resources, and may be on some context information of the request (see below), a principal will be granted or denied access.

In some cases, access control decision needs to take into account not only “what operation is performed on what resource by whom” but also how drastic the change, if any, is going to happen. A simplified hypothetical example can be a rule that allows only an attending physician to double the dose of some medicine prescribed to a patient.

Type of access operations on “secured resources” is a factor in access control decisions. This RFP uses a common model, in which any complex operation on resources is considered as a serializable sequence of elementary operations “create”, “read”, “write”, “delete”, "use."

In order for the described access control logic to be useful, an interface to the logic that will allow defining access control rules is needed. Such an interface should allow to express access control rules in terms of Principal Privilege Attributes, secured resources, operations on those resources, and possibly other factors listed in Section 6.6 (Optional Requirements).

A context of client←→target object interaction is also of interest to access control decisions. Access control logic can take into account time of access to the resource and location of the requesting principal.

The RFP is looking for a solution where individual applications, or target objects, play the most minimal role possible in the realization of an enterprise security policy. Optimally, each application's, or object's, contribution to security will be limited to requesting and enforcing access control decisions - without knowing or caring about how the decisions are made. This then allows the definition, implementation and management of each application, or object, and the enterprise-specific security policy to be orthogonal.

6.3 Relationship to Existing OMG Specifications

A facility asked in this RFP is sought to reuse CORBAservices and CORBAfacilities extensively. The CORBA Security service is expected to be the main building foundation for the facility.

6.4 Related Documents and Standards

- Object Management Group, CORBAservices: Common Object Services Specification, Security Service Specification
- Person Identification Service (PIDS) specification – work in progress
- OMG Product Data Management Enablers, sections 2.1, 2.2 and 2.6.
- Draft "CORBAmed Security White Paper" OMG document number: corbamed/97-11-03
- Green paper on "Applicability of CORBA Security to the Healthcare Problem Domain" OMG document number: corbamed/97-09-11
- Privacy and Confidentiality: Access Control in Healthcare Information Systems, CareFlow|Net, Inc. white paper (http://www.careflow.com/docs/whitepaper/AccessControl.html).

6.5 Mandatory Requirements

1. Proposals *shall* use the CORBA Security service credentials as the source for identifying caregivers' privileges. The CORBA Security service provides a foundation for the intended facility.

2. Proposals *shall* provide the ability to define secured resource categories -- including CORBA objects and other resources as it discussed in section 6.2 -- and the ability for an application to discover to which secured resource category a CORBA object or other resource belongs. Proposals *shall* provide the ability to state and evaluate

policies governing the following minimal set of operations on secured resources: create, read, write, use and delete.

3. Proposals *shall* provide an interface for defining access control rules for secured resources based on credentials as defined in the CORBA Security Specification. Examples of access control rules are given in section 6.1.

4. Proposals *shall* define a specific set of Healthcare secured resources. Examples of such resources might include demographic information, laboratory results, HIV status etc.

5. Proposals *shall* provide an interface to an access control decision facility that may be used to request access control decisions

6.6 Optional Requirements

1. Proposals *may* provide the ability for secured resources -- including resources that are not CORBA objects -- to be grouped for the purpose of defining access control rules.

2. Proposals *may* provide an interface for defining access control rules based on attributes of the Principal in addition to those defined in CORBA Security service.

3. Proposals *may* provide an interface that extends the definition of access control rules to include context sensitive access control based on

   - the day and time when the resource is accessed
   - the location of an invoking principal
   - the values of request parameters

4. Proposals *may* provide an interface that extends the definition of access control rules to include notion of relationship between a patient and a caregiver.

5. Proposals *may* include a reference object model for the healthcare domain that provides a sufficient foundation for access control decision logic.

6. Proposals *may* provide an interface that permits management of the policy, which controls how multiple access control policy decisions governing access to the same resource are reconciled.

6.7 Issues to be discussed

Proposals should discuss how new CORBAmed specifications will employ the submitted specification.

Proposals should discuss how existing CORBAmed specifications are to be modified.

Proposals should discuss scalability and performance of the proposal.

Proposals should discuss mechanisms provided for extensibility.

6.8 Evaluation Criteria

The following criteria will be applied during the evaluation process:

- Consistency with the CORBA Security service ideology.
- Degree of security awareness required of applications, which use the proposed solution.
- Scalability of the proposed solutions.
- Extensibility of the proposed solutions.

6.9 Other information unique to this RFP

6.9.1 Terminology

This section defines some words and expressions in order to have common understanding of them. Terminology not defined in this section is assumed to have meaning specified elsewhere in the OMG official documents.

The **Principal role** is one of the defined CORBA Security attributes that a client acting on behalf of that principal might have in its credentials.

The **content-based security** considers content of data manipulated in client←→target object interactions as if it were security relevant. For example, content-based security allows enforcement of access control and other security policies based on method input argument values

and/or return result values.

The **context-based security** allows making security policy decisions based on such context of client←→target object interactions as location of the initiating client and time of the request.

6.10 RFP Timetable

The timetable for this RFP is given below. Note that the TF may, in certain circumstances, extend deadlines while the RFP is running, or may elect to have more than one revised submission step. The latest timetable can always be found in the Member Services section of OMG's Web page (URL http://www.omg.org/)

Approx Day	**Event or** *Activity*	**Actual Date**
	Preparation of RFP by TF	
	Approval of RFP by Architecture Board *Review by TC ("Three week rule")*	
0	TC votes to issue RFP	Fri Feb 13, 1998
94	LOI to submit to RFP due	Mon May 18, 1998
150	Initial submissions due	Mon Aug 24, 1998
164	Voter registration closes	Mon Sep 7, 1998
171	Initial submission presentations Seattle,WA, USA	Mon Sep 14, 1998
	Preliminary evaluation by TF	
206	Revised submissions due	Mon Oct 19, 1998
227	Revised submission presentations Burlingame, CA, USA	Mon Nov 9, 1998
	Final evaluation and selection by TF *Recommendation to AB and TC*	
	Approval by Architecture Board *Review by TC ("Three week rule")*	
360	TC votes to recommend specifications	February, 1999
390	BOD votes to adopt specifications	March, 1999