

# 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 Security Framework Request For Proposal

OMG Document: corbamed/97-11-04

### DRAFT 0.1

**Submissions due:** <month name e.g. January> <day>, <year>

#### Objective of this RFP

The complexity of the healthcare security problem domain requires exercising more sophisticated security policies rather than the general policies 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 security policies in a uniform and standard way.

This RFP solicits proposals for healthcare security frameworks based on the CORBA Security service. Such a framework will provide a uniform way for healthcare systems to enforce domain-oriented security policies.

For further details see Chapter 6 of this document.

## **6.0 Specific Requirements on Proposals**

### **6.1 Problem Statement**

CORBA services and CORBA facilities provide a general-purpose infrastructure for developing distributed object systems in a broad range of specialized vertical domains. The CORBA Security service is one of this kind.

The CORBA Security service is meant to provide a versatile set of mechanisms to enforce diverse security models. Some of these models 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.

This RFP seeks to provide a security framework based on CORBA Services and CORBA Facilities, specifically on the CORBA Security service, that will allow exercising healthcare domain-oriented complex security policies in a portable and interoperable fashion across healthcare enterprises.

### **6.2 Scope of Proposals Sought**

Healthcare Security Framework (HSF) is sought to be a framework that will allow application systems to be unaware of advanced security policies existing in healthcare enterprises where those systems are deployed. The first step in designing HSF is to find solutions for currently clarified problems. Other iterations of HSF will address issues that are subtle or do not even exist today.

The main challenge of expressing real-life healthcare security constraints in terms of OMA-based specifications layered on top of existing CORBA Security is a necessity to enforce, and administrate finer granularity security policies. The granularity of such policies has to be up to the level of method input arguments and output results. For a discussion of this issue, see “CORBAmed Security White Paper” listed in section 6.4.

### 6.3 Relationship to Existing OMG Specifications

HSF is sought to reuse CORBA services and CORBA facilities extensively. The CORBA Security service is expected to be the main building foundation for the framework.

### 6.4 Related Documents and Standards

- Object Management Group, CORBA services: Common Object Services Specification, Security Service Specification
- Person Identification Service (PIDS) specification – work in progress
- 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

### 6.5 Mandatory Requirements

- Proposals *shall* reuse the CORBA Security service as a foundation for the intended framework and honor the ideology of the service design.
- Proposals *shall* provide capabilities of enforcing fine granularity security policies on the following entity types:
  - Domain::Interface::Method input argument values
  - Domain::Interface::Method output argument values and return result value
- Proposals *shall* provide capabilities of enforcing fine granularity security policies, listed in this subsection, on minimally security-aware applications. I.e. an application *shall* not do more than consulting with decision objects that are external to the application.
- The list of types of security policies that proposals *shall* provide is the same as the CORBA Security service specifies.
- Proposals *shall* provide an administrator interface to manage such policies.

## 6.6 Optional Requirements

- Proposals *may* provide capabilities of enforcing and therefore administrating fine granularity security policies on the following entity types:
  - Day and time when service is accessed
  - Location of an invoking principal
- Proposals *may* support the ability to specify security policy administration capabilities that utilize the notion of person identification and/or traits associated with it, according to the final specification of the Person Identification Service that is soon to be adopted.

## 6.7 Issues to be discussed

Proposals *should* discuss how new CORBAmed specifications will employ HSF.

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

## 6.8 Evaluation Criteria

The following criteria will be applied during the evaluation process:

- Whether the proposals are consistent with the CORBA Security service ideology.
- Whether the proposals allow enforcement of security policies described in the “Mandatory Requirements” section on security unaware applications.
- Whether the proposed solutions are potentially scalable.

## 6.9 Other information unique to this RFP

TBD

### 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/>)

<b>Approx Day</b>	<b>Event or Activity</b>	<b>Actual Date</b>
	<i>Preparation of RFP by TF</i>	
	<i>Approval of RFP by Architecture Board Review by TC (“Three week rule”)</i>	
0	TC votes to issue RFP	<approximate month>
60	LOI to submit to RFP due	January <day>, <year>
120	Initial submissions due	January <day>, <year>
134	Voter registration closes	January <day>, <year>
141	Initial submission presentations	January <day>, <year>
	<i>Preliminary evaluation by TF</i>	
240	Revised submissions due	January <day>, <year>
261	Revised submission presentations	January <day>, <year>
	<i>Final evaluation and selection by TF Recommendation to AB and TC</i>	
	<i>Approval by Architecture Board Review by TC (“Three week rule”)</i>	
330	TC votes to recommend specifications	<approximate month>
360	BOD votes to adopt specifications	<approximate month>