

Object Management Group

140 Kendrick Street
Building A Suite 300
Needham, MA 02494
USA

Telephone: +1-781-444-0404

Facsimile: +1-781-444-0320

Request for Proposal

Reference Models of Business Processes for Financial Services

OMG Document: **finance/2007-03-01**

Letters of Intent due: <month> <day>, <year>

Submissions due: <month> <day>, <year>

Objective of this Request for Proposal (RFP)

Modeling the financial processes involved in account opening and funds transfer in a formal way is a first step in a broad industry effort to make business processes across the financial services industry more efficient and secure.

Reference models for these processes are intended to elucidate the security issues across inter-enterprise financial services networks, and to provide an architectural framework for further elaboration of financial processes that create, carry or consume sensitive data.

The financial services industry and their suppliers will use these reference models to collaboratively identify opportunities to improve security policy and controls. In particular, it is expected that redundancies and inefficiencies in existing processes, often the cause of security issues, will be addressed.

This RFP, issued by the Finance Domain Task Force (FDTF) of the OMG, therefore solicits proposals for the following:

- the definition of a metamodel for financial processes, focusing on security and privacy of information; such a metamodel captures concepts and relationships, and forms the basis for expressing reference models;
- the definition of a UML profile for financial processes, intended to help guide the use of a UML tool in manipulating the models;
- the definition of standard reference models for account opening and funds transfer¹ processes, based on the metamodel; and
- the definition of an architectural framework based on the reference models, intended to identify opportunities for improved security and privacy mechanisms, protocols, and policies.

This RFP reflects substantial feedback from over one hundred firms in the financial services industry in conclaves that were held in New York, St. Louis, San Francisco, London, and Rome in the process of gathering inputs to the OMG RFI, 'High Level Models of Financial Business Processes', <http://www.omg.org/cgi-bin/doc?finance/2006-03-01>, issued by the FDTF [RFI].

1.0 Introduction

1.1 Goals of OMG

The Object Management Group (OMG) is the world's largest software consortium with an international membership of vendors, developers, and end users. Established in 1989, its mission is to help computer users solve enterprise integration problems by supplying open, vendor-neutral portability, interoperability and reusability specifications based on Model Driven Architecture (MDA). MDA defines an approach to IT system specification that separates the specification of system functionality from the specification of the implementation of that functionality on a specific technology platform, and provides a set of guidelines for structuring specifications expressed as models. OMG has established numerous widely used standards such as OMG IDL[IDL], CORBA[CORBA], Realtime CORBA [CORBA], GIOP/IIOP[CORBA], UML[UML], MOF[MOF], XMI[XMI] and CWM[CWM] to name a few significant ones.

1.2 Organization of this document

The remainder of this document is organized as follows:

¹ 'Funds Transfers' for the purpose of this RFP are those among financial institutions. As will be explained later in this document, respondents can optionally present models for corporate-to-corporate or corporate-to-financial institution funds transfers.

Chapter 2 - *Architectural Context* - background information on OMG's Model Driven 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, requirements and optional features, issues to be discussed, evaluation criteria, and timetable that apply specifically to this RFP.

Appendix A – *References and Glossary Specific to this RFP*

Appendix B – *General References and Glossary*

1.3 Conventions

The key words "**must**", "**must not**", "**required**", "**shall**", "**shall not**", "**should**", "**should not**", "**recommended**", "**may**", and "**optional**" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1.4 Contact Information

Questions related to the OMG's technology adoption process may be directed to omg-process@omg.org. General questions about this RFP may be sent to responses@omg.org.

OMG documents (and information about the OMG in general) can be obtained from the OMG's web site (<http://www.omg.org/>). OMG documents may also be obtained by contacting OMG at documents@omg.org. Templates for RFPs (this document) and other standard OMG documents can be found at the *OMG Template Downloads Page* at http://www.omg.org/technology/template_download.htm

2.0 Architectural Context

MDA provides a set of guidelines for structuring specifications expressed as models and the mappings between those models. The MDA initiative and the standards that support it allow the same model specifying business system or application functionality and behavior to be realized on multiple platforms. MDA enables different applications to be integrated by explicitly relating their models; this facilitates integration and interoperability and supports system evolution (deployment choices) as platform technologies change. The three primary goals of MDA are portability, interoperability and reusability.

Portability of any subsystem is relative to the subsystems on which it depends. The collection of subsystems that a given subsystem depends upon is often loosely called the *platform*, which supports that subsystem. Portability – and reusability – of such a subsystem is enabled if all the subsystems that it depends upon use standardized interfaces (APIs) and usage patterns.

MDA provides a pattern comprising a portable subsystem that is able to use any one of multiple specific implementations of a platform. This pattern is repeatedly usable in the specification of systems. The five important concepts related to this pattern are:

1. *Model* - A model is a representation of a part of the function, structure and/or behavior of an application or system. A *representation* is said to be *formal* when it is based on a language that has a well-defined form (“syntax”), meaning (“semantics”), and possibly rules of analysis, inference, or proof for its constructs. The syntax may be graphical or textual. The semantics might be defined, more or less formally, in terms of things observed in the world being described (e.g. message sends and replies, object states and state changes, etc.), or by translating higher-level language constructs into other constructs that have a well-defined meaning. The optional rules of inference define what unstated properties you can deduce from the explicit statements in the model. In MDA, a *representation* that is not *formal* in this sense is not a model. Thus, a diagram with boxes and lines and arrows that is not supported by a definition of the meaning of a box, and the meaning of a line and of an arrow is not a model—it is just an informal diagram.
2. *Platform* – A set of subsystems/technologies that provide a coherent set of functionality through interfaces and specified usage patterns that any subsystem that depends on the platform can use without concern for the details of how the functionality provided by the platform is implemented.
3. *Platform Independent Model (PIM)* – A model of a subsystem that contains no information specific to the platform, or the technology that is used to realize it.
4. *Platform Specific Model (PSM)* – A model of a subsystem that includes information about the specific technology that is used in the realization of that subsystem on a specific platform, and hence possibly contains elements that are specific to the platform.
5. *Mapping* – Specification of a mechanism for transforming the elements of a model conforming to a particular metamodel into elements of another model that conforms to another (possibly the same) metamodel. A mapping may be expressed as associations, constraints, rules, templates with parameters that must be assigned during the mapping, or other forms yet to be determined.

For example, in case of CORBA the platform is specified by a set of interfaces and usage patterns that constitute the CORBA Core Specification [CORBA]. The CORBA platform is independent of operating systems and programming languages. The OMG Trading Object Service specification [TOS] (consisting of interface specifications in OMG Interface Definition Language (OMG IDL)) can be considered to be a PIM from the viewpoint of CORBA, because it is independent of operating systems and programming languages. When the IDL to C++ Language Mapping specification is applied to the Trading Service PIM, the C++-specific result can be considered to be a PSM for the Trading Service, where the platform is the C++ language and the C++ ORB implementation. Thus the IDL to C++ Language Mapping specification [IDLC++] determines the mapping from the Trading Service PIM to the Trading Service PSM.

Note that the Trading Service model expressed in IDL is a PSM relative to the CORBA platform too. This highlights the fact that platform-independence and platform-specificity are relative concepts.

The UML Profile for EDOC specification [EDOC] is another example of the application of various aspects of MDA. It defines a set of modeling constructs that are independent of middleware platforms such as EJB [EJB], CCM [CCM], MQSeries [MQS], etc. A PIM based on the EDOC profile uses the middleware-independent constructs defined by the profile and thus is middleware-independent. In addition, the specification defines formal metamodels for some specific middleware platforms such as EJB, supplementing the already-existing OMG metamodel of CCM (CORBA Component Model). The specification also defines mappings from the EDOC profile to the middleware metamodels. For example, it defines a mapping from the EDOC profile to EJB. The mapping specifications facilitate the transformation of any EDOC-based PIM into a corresponding PSM for any of the specific platforms for which a mapping is specified.

Continuing with this example, one of the PSMs corresponding to the EDOC PIM could be for the CORBA platform. This PSM then potentially constitutes a PIM, corresponding to which there would be implementation language specific PSMs derived via the CORBA language mappings, thus illustrating recursive use of the Platform-PIM-PSM-Mapping pattern.

Note that the EDOC profile can also be considered to be a platform in its own right. Thus, a model expressed via the profile is a PSM relative to the EDOC platform.

An analogous set of concepts apply to Interoperability Protocols wherein there is a PIM of the payload data and a PIM of the interactions that cause the data to find its way from one place to another. These then are realized in specific ways for specific platforms in the corresponding PSMs.

Analogously, in case of databases there could be a PIM of the data (say using the Relational Data Model), and corresponding PSMs specifying how the data is

actually represented on a storage medium based on some particular data storage paradigm etc., and a mapping from the PIM to each PSM.

OMG adopts standard specifications of models that exploit the MDA pattern to facilitate portability, interoperability and reusability, either through ab initio development of standards or by reference to existing standards. Some examples of OMG adopted specifications are:

1. *Languages* – e.g. IDL for interface specification, UML for model specification, OCL for constraint specification, etc.
2. *Mappings* – e.g. Mapping of OMG IDL to specific implementation languages (CORBA PIM to Implementation Language PSMs), UML Profile for EDOC (PIM) to CCM (CORBA PSM) and EJB (Java PSM), CORBA (PSM) to COM (PSM) etc.
3. *Services* – e.g. Naming Service [NS], Transaction Service [OTS], Security Service [SEC], Trading Object Service [TOS] etc.
4. *Platforms* – e.g. CORBA [CORBA].
5. *Protocols* – e.g. GIOP/IIOP [CORBA] (both structure and exchange protocol), [XMI] (structure specification usable as payload on multiple exchange protocols).
6. *Domain Specific Standards* – e.g. Data Acquisition from Industrial Systems (Manufacturing) [DAIS], General Ledger Specification (Finance) [GLS], Air Traffic Control (Transportation) [ATC], Gene Expression (Life Science Research) [GE], Personal Identification Service (Healthcare) [PIDS], etc.

For an introduction to MDA, see [MDAa]. For a discourse on the details of MDA please refer to [MDAc]. To see an example of the application of MDA see [MDAb]. For general information on MDA, see [MDAd].

Object Management Architecture (OMA) is a distributed object computing platform architecture within MDA that is related to ISO's Reference Model of Open Distributed Processing RM-ODP[RM-ODP]. CORBA and any extensions to it are based on OMA. For information on OMA see [OMA].

3.0 Adoption Process

3.1 Introduction

OMG adopts specifications by explicit vote on a technology-by-technology basis. The specifications selected each satisfy the architectural vision of MDA.

OMG bases its decisions on both business and technical considerations. Once a specification adoption is finalized by OMG, it is made available for use by both OMG members and non-members alike.

Request for Proposals (RFP) are issued by a *Technology Committee (TC)*, typically upon the recommendation of a *Task Force (TF)* and duly endorsed by the *Architecture Board (AB)*.

Submissions to RFPs are evaluated by the TF that initiated the RFP. Selected specifications are *recommended* to the parent TC after being *reviewed* for technical merit and consistency with MDA and other adopted specifications and *endorsed* by the AB. The parent TC of the initiating TF then votes to *recommend adoption* to the OMG Board of Directors (BoD). The BoD acts on the recommendation to complete the adoption process.

For more detailed information on the adoption process see the *Policies and Procedures of the OMG Technical Process [P&P]* and the *OMG Hitchhiker's Guide [Guide]*. In case of any inconsistency between this document and the [P&P] in all cases the [P&P] shall prevail.

3.2 Steps in the Adoption Process

A TF, its parent TC, the AB and the Board of Directors participate in a collaborative process, which typically takes the following form:

- *Development and Issuance of RFP*

RFPs are drafted by one or more OMG members who are interested in the adoption of a standard in some specific area. The draft RFP is presented to an appropriate TF, based on its subject area, for approval and recommendation to issue. The TF and the AB provide guidance to the drafters of the RFP. When the TF and the AB are satisfied that the RFP is appropriate and ready for issuance, the TF recommends issuance to its parent TC, and the AB endorses the recommendation. The TC then acts on the recommendation and issues the RFP.

- *Letter of Intent (LOI)*

A Letter of Intent (LOI) must be submitted to the OMG signed by an officer of the member organization, which intends to respond to the RFP, confirming the organization's willingness to comply with OMG's terms and conditions, and commercial availability requirements. (See section 4.3 for more information.). In order to respond to an RFP the respondent must be a member of the TC that issued the RFP.

- *Voter Registration*

Interested OMG members, other than Trial, Press and Analyst members may participate in specification selection votes in the TF for an RFP. They

may need to register to do so, if so stated in the 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. Member organizations that 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 first meeting of the TF after the deadline. Initial Submissions are expected to be complete enough to provide insight on the technical directions and content of the proposals.

- *Revision Phase*

During this time submitters have the opportunity to revise their Submissions, if they so choose.

- *Revised Submissions*

Revised Submissions are due by a specified deadline. Submitters again normally present their proposals at the next meeting of the TF after the deadline. (Note that there may be more than one Revised Submission deadline. The decision to extend this deadline is made by the registered voters for that RFP.)

- *Selection Votes*

When the registered voters for the RFP believe that they sufficiently understand the relative merits of the Revised Submissions, a selection vote is taken. The result of this selection vote is a recommendation for adoption to the TC. The AB reviews the proposal for MDA compliance and technical merit. An endorsement from the AB moves the voting process into the issuing Technology Committee. An eight-week voting period ensues in which the TC votes to recommend adoption to the OMG Board of Directors (BoD). The final vote, the vote to adopt, is taken by the BoD and is based on technical merit as well as business qualifications. The resulting draft standard is called the *Adopted Specification*.

- *Business Committee Questionnaire*

The submitting members whose proposal is recommended for adoption need to submit their response to the BoD Business Committee Questionnaire [BCQ] detailing how they plan to make use of and/or make the resulting standard available in products. If no organization commits to make use of the standard, then the BoD will typically not act on the recommendation to adopt the standard. So it is very important to fulfill this requirement.

- *Finalization*

A Finalization Task Force (FTF) is chartered by the TC that issued the RFP, to prepare an *adopted* submission for publishing as a formal, publicly available specification. Its responsibility includes production of one or more prototype implementations and fixing any problems that are discovered in the process. This ensures that the final available standard is actually implementable and has no show-stopping bugs. Upon completion of its activity the FTF recommends adoption of the resulting draft standard called the *Available Specification*. The FTF must also provide evidence of the existence of one or more prototype implementations. The parent TC acts on the recommendation and recommends adoption to the BoD. OMG Technical Editors produce the *Formal Published Specification* document based on this *Available Specification*.

- *Revision*

A Revision Task Force (RTF) is normally chartered by a TC, after the FTF completes its work, to manage issues filed against the *Available Specification* by implementers and users. The output of the RTF is a revised specification reflecting minor technical changes.

3.3 Goals of the evaluation

The primary goals of the TF evaluation are to:

- Provide a fair and open process
- Facilitate critical review of the submissions by members of OMG
- Provide feedback to submitters enabling them to address concerns in their revised submissions
- Build consensus on acceptable solutions
- Enable voting members to make an informed selection decision

Submitters are expected to actively contribute to the evaluation process.

4.0 Instructions for Submitters

4.1 OMG Membership

To submit to an RFP issued by the Platform Technology Committee the submitter or submitters must be either Platform or Contributing members on the date of the submission deadline, while for Domain Technology RFPs the submitter or submitters must be either Contributing or Domain members.

Submitters sometimes choose to name other organizations 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 organizations thus named.

4.2 Submission Effort

An RFP submission may require significant effort in terms of document preparation, presentations to the issuing 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 the submitting organization signifying its intent to respond to the RFP and confirming the 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 the submitting organization for receipt of all subsequent information regarding this RFP and the 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 <__organization required__> (the organization) 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/06-03-02.

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

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

<__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 is available separately as an OMG document omg/06-03-02.

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 Committees; 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 organizations. 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 organizations 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 Access to Intellectual Property Rights

OMG will not adopt a specification if OMG is aware of any submitter, member or third party which holds a patent, copyright or other intellectual property right (collectively referred to in this policy statement as "IPR") which might be infringed by implementation or recommendation of such specification, unless OMG believes that such IPR owner will grant a license to organizations (whether OMG members or not) on non-discriminatory and commercially reasonable terms which wish to make use of the specification. Accordingly, the submitter must certify that it is not aware of any claim that the specification infringes any IPR of a third party or that it is aware and believes that an appropriate non-discriminatory license is available from that third party. Except for this certification, the submitter will not be required to make any other warranty, and specifications will be offered by OMG for use "as is". If the submitter owns IPR to which an use of a specification based upon its submission would necessarily be subject, it must certify to the Business Committee that it will make a suitable license available to any user on non- discriminatory and commercially reasonable terms, to permit development and commercialization of an implementation that includes such IPR.

It is the goal of the OMG to make all of its technology available with as few impediments and disincentives to adoption as possible, and therefore OMG strongly encourages the submission of technology as to which royalty-free licenses will be available. However, in all events, the submitter shall also certify that any necessary license will be made available on commercially reasonable, non-discriminatory terms. The submitter is responsible for disclosing in detail all known restrictions, placed either by the submitter or, if known, others, on technology necessary for any use 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 license 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 Complete proposals

A submission must propose full specifications for all of the relevant requirements detailed in Chapter 6 of this RFP. Submissions that do not present complete proposals may be at a disadvantage.

Submitters are highly encouraged to propose solutions to any optional requirements enumerated in Chapter 6.

4.5.2 Additional specifications

Submissions may include additional specifications for items not covered by the RFP that 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.

4.5.3 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 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 confidential or proprietary information of any kind will be accepted in a submission to this RFP.

4.7 Copyright Waiver

Every submission document must contain: (i) a waiver of copyright for unlimited duplication by the OMG, and (ii) a limited waiver of copyright that allows each OMG member to make up to fifty (50) copies of the document for review purposes only. See Section 4.9.2 for recommended language.

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 in 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 managing the evaluation process, the technical viability of their proposal. OMG will favor proposals based on technology for which sufficient relevant experience has been gained.

4.9 Format of RFP Submissions

This section presents the structure of a submission in response to an RFP. *All submissions* must contain the elements itemized in section 4.9.2 below before they can be accepted as a valid response for evaluation or a vote can be taken to recommend for adoption.

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 key words "**must**", "**must not**", "**required**", "**shall**", "**shall not**", "**should**", "**should not**", "**recommended**", "**may**", and "**optional**" shall be used in the submissions with the meanings as described in RFC 2119 [RFC2119].

4.9.2 Required Outline

A three-part structure for submissions is required. Part I is non-normative, providing information relevant to the evaluation of the proposed specification. Part II is normative, representing the proposed specification. Specific sections like Appendices may be explicitly identified as non-normative in Part II. Part III is normative specifying changes that must be made to previously adopted

specifications in order to be able to implement the specification proposed in Part II.

PART I

- The name of the RFP that the submission is responding to.
- List of OMG members making the submission (see 4.1) listing exactly which members are making the submission, so that submitters can be matched with LOI responders and their current eligibility can be verified.
- Copyright waiver (see 4.7), in a form acceptable to the OMG.

One acceptable form is:

“Each of the entities listed above: (i) grants to the Object Management Group, Inc. (OMG) a nonexclusive, royalty-free, paid up, worldwide license to copy and distribute this document and to modify this document and distribute copies of the modified version, and (ii) grants to each member of the OMG a nonexclusive, royalty-free, paid up, worldwide license to make up to fifty (50) copies of this document for internal review purposes only and not for distribution, and (iii) has agreed that no person shall be deemed to have infringed the copyright in the included material of any such copyright holder by reason of having used any OMG specification that may be based hereon or having conformed any computer software to such specification.”

If you wish to use some other form you must get it approved by the OMG legal counsel before using it in a submission.

- For each member making the submission, an individual contact point who is authorized by the member to officially state the member’s position relative to the submission, including matters related to copyright ownership, etc. (see 4.3)
- Overview or guide to the material in the submission
- Overall design rationale (if appropriate)
- Statement of proof of concept (see 4.8)
- Resolution of RFP requirements and requests

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

In addition, if the 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

The contents of this part should be structured based on the template found in [FORMS] and should contain the following elements as per the instructions in the template document cited above:

- Scope of the proposed specification
- Proposed conformance criteria

Submissions should propose appropriate conformance criteria for implementations.

- Proposed normative references

Submissions should provide a list of the normative references that are used by the proposed specification

- Proposed list of terms and definitions

Submissions should provide a list of terms that are used in the proposed specification with their definitions.

- Proposed list of symbols

Submissions should provide a list of special symbols that are used in the proposed specification together with their significance

- Proposed specification.

PART III

- 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.

4.10 How to Submit

Submitters should send an electronic version of their submission to the *RFP Submissions Desk* (omg-documents@omg.org) at OMG Headquarters by 5:00 PM U.S. Eastern Standard Time (22:00 GMT) on the day of the Initial and Revised Submission deadlines. Acceptable formats are Postscript, ASCII, PDF, Adobe FrameMaker, Microsoft Word, and WordPerfect. However, it should be

noted that a successful (adopted) submission must be supplied to OMG's technical editors in FrameMaker source format, using the most recent available OMG submission template (see [FORMS]). The AB will not endorse adoption of any submission for which appropriately formatted FrameMaker sources are not submitted to OMG; 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 be prepared to send a single hardcopy version of their submission, if requested by OMG staff, to the attention of the "RFP Submissions Desk" at the main OMG address shown on the first page of this RFP.

5.0 General Requirements on Proposals

5.1 Requirements

- 5.1.1 Submitters are encouraged to express models using OMG modeling languages such as UML, MOF, CWM and SPEM (subject to any further constraints on the types of the models and modeling technologies specified in Chapter 6 of this RFP). Submissions containing models expressed via OMG modeling languages shall be accompanied by an OMG XMI [XMI] representation of the models (including a machine-readable copy). A best effort should be made to provide an OMG XMI representation even in those cases where models are expressed via non-OMG modeling languages.
- 5.1.2 Chapter 6 of this RFP specifies whether PIM(s), PSM(s), or both are being solicited. If proposals specify a PIM and corresponding PSM(s), then the rules specifying the mapping(s) between the PIM and PSM(s) shall either be identified by reference to a standard mapping or specified in the proposal. In order to allow possible inconsistencies in a proposal to be resolved later, proposals shall identify whether the mapping technique or the resulting PSM(s) are to be considered normative.
- 5.1.3 Proposals shall be *precise* and *functionally complete*. All relevant assumptions and context required for implementing the specification shall be provided.
- 5.1.4 Proposals shall specify *conformance criteria* that clearly state what features all implementations must support and which features (if any) may *optionally* be supported.
- 5.1.5 Proposals shall *reuse* existing OMG and other standard specifications in preference to defining new models to specify similar functionality.

- 5.1.6 Proposals shall justify and fully specify any *changes or extensions* required to existing OMG specifications. In general, OMG favors proposals that are *upwards compatible* with existing standards and that minimize changes and extensions to existing specifications.
- 5.1.7 Proposals shall factor out functionality that could be used in different contexts and specify their models, interfaces, etc. separately. Such *minimalism* fosters re-use and avoids functional duplication.
- 5.1.8 Proposals shall use or depend on other specifications only where it is actually necessary. While re-use of existing specifications to avoid duplication will be encouraged, proposals should avoid gratuitous use.
- 5.1.9 Proposals shall be *compatible* with and *usable* with existing specifications from OMG and other standards bodies, as appropriate. Separate specifications offering distinct functionality should be usable together where it makes sense to do so.
- 5.1.10 Proposals shall preserve maximum *implementation flexibility*. Implementation descriptions should not be included and proposals shall not constrain implementations any more than is necessary to promote interoperability.
- 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's Reference Model of Open Distributed Processing [RM-ODP]. Where such compatibility is not achieved, or is not appropriate, 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 specification 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 elements that are introduced by the proposal?
 - Which accesses to security-sensitive elements must be subject to security policy control?
 - Does the proposed service or facility need to be security aware?

- What default policies (e.g., for authentication, audit, authorization, message protection etc.) should be applied to the security sensitive elements introduced by the proposal? Of what security considerations must the implementers of your proposal be aware?

The OMG has adopted several specifications, which cover different aspects of security and provide useful resources in formulating responses. [CSIV2] [SEC] [RAD].

- 5.1.14 Proposals shall specify the degree of internationalization support that they provide. The degrees of support are as follows:
- a) Uncategorized: Internationalization has not been considered.
 - b) Specific to <region name>: The proposal supports the customs of the specified region only, and is not guaranteed to support the customs of any other region. Any fault or error caused by requesting the services outside of a context in which the customs of the specified region are being consistently followed is the responsibility of the requester.
 - c) Specific to <multiple region names>: The proposal supports the customs of the specified regions only, and is not guaranteed to support the customs of any other regions. Any fault or error caused by requesting the services outside of a context in which the customs of at least one of the specified regions are being consistently followed is the responsibility of the requester.
 - d) Explicitly not specific to <region(s) name>: The proposal does not support the customs of the specified region(s). Any fault or error caused by requesting the services in a context in which the customs of the specified region(s) are being followed is the responsibility of the requester.

5.2 Evaluation criteria

Although the OMG adopts model-based specifications and not implementations of those 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 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 Conformance: Inspectability and Testability

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

5.2.5 Standardized Metadata

Where proposals incorporate metadata specifications, usage of OMG standard XMI metadata [XMI] representations must be provided as this allows specifications to be easily interchanged between XMI compliant tools and applications. Since use of XML (including XMI and XML/Value [XML/Value]) is evolving rapidly, the use of industry specific XML vocabularies (which may not be XMI compliant) is acceptable where justified.

6.0 Specific Requirements on Proposals

After the RFI was issued, the Finance Domain Task Force (FDTF) of the OMG convened conclaves in the locations listed in the Objective section at the start of this document. Members of financial institutions as well as from the vendor community responded in large numbers to the invitation to jointly identify key security issues and discuss the application of a model-based framework to addressing those issues. This RFP is based on the inputs received during the conclaves.

Participants in the conclaves observed that the security of current financial processes can be enhanced by eliminating redundancies and increasing efficiency. Indeed, information is often exchanged multiple times in the same financial transaction, exposing the data more often than is required and increasing the possibility of interception or compromise.

To focus the activity, the account opening and funds transfer processes were identified by the participants as the most promising areas for improvement, as well as being representative of the larger set of financial processes. Specific security concerns relating to those processes were then discussed.

6.1 Problem Statement

The financial services industry conducts electronic transactions using processes that mimic the paper-based exchanges that were executed before the availability of IP-based networks. Given the different security issues and characteristics of electronic transactions, the inefficiencies and redundancies of these mimicked processes raise the potential for security compromises.

In response, the financial services industry and its vendor community have invested considerable resources to define standards to improve the security, confidentiality, and audit-ability of the electronic movement and storage of sensitive data. Though these activities are valuable to the financial industry, the functional protocols resulting from the work still tend to be bulwarks against security problems stemming from pre-IP age business processes that are inherently unsuitable to the security requirements of an electronically connected world.

Unfortunately, variations in the implementation of the security mechanisms and the processes themselves have introduced vulnerabilities and increased information security risks for the industry as a whole.

The industry has agreed that a solution to these deficiencies is of vital importance and this RFP is intended to address those concerns. The ultimate goal of standardizing process models for inter-enterprise business transactions that create, carry, and consume sensitive data is to make the use of the

functional security protocols more effective by providing a coherent framework for their application.

This is the natural evolution of processes in the business-to-business (B2B) space: the first wave of automation of such processes focused on mimicking existing processes. The next wave will enhance the processes themselves so that they use technology more optimally and uniformly and take advantage of modeling technology to ensure that the processes are globally understood.

The FDTF believes that the first step in accomplishing the goal of industry agreed-upon standards is the development of standard reference models for some key business processes in the financial services industry. These reference models will provide a shared and common framework for the analysis of security issues utilizing functional protocols. That analysis should also reveal gaps in the existing functional protocols that need to be addressed.

This RFP is a first and crucial step in the process of using MDA for re-engineering processes in order to reduce sensitive data vulnerability and associated risks and liabilities. This first step entails re-thinking account opening and funds transfers, and modeling the resulting re-engineered processes, taking into account security issues at the business level.

Subsequent RFPs will initiate follow-on steps that map these business models to technical protocols and solutions.

The real value of defining these initial reference models is in providing to the industry commonly understood concepts and processes with clear, formally-modeled semantics as a framework for the analysis of security issues.

The models that are created will be reviewed by domain-specific standards organizations, such as ISO TC68 (Financial Services), the Financial Services Technical Consortium (FSTC), and others.

It must be emphasized that the basis for the models will be financial processes (specifically account opening and funds transfer) as they exist today, but as was stated earlier, the models that the FDTF intends to formally specify will be for the re-engineered processes. In addition, as the resulting models are expected to provide a blueprint for other financial processes, the creation of a metamodel and a UML profile for financial services is a goal of this RFP as well.

6.1.1 Information Security Issues

This section documents the primary security issues identified in the RFI data gathering process. It captures the security concerns related to the execution of existing financial service processes, provides a framework for their analysis, and informs the effort to re-engineer these processes to address the security concerns that were raised.

6.1.1.1 Primary security issues identified

As mentioned above, electronic data transmission as practiced today tends to mimic the way we have traditionally conducted paper-based commerce. When we move an information-packed paper form from place to place, all of the information on the form moves with it. Electronic data transmission imitates this pattern.

When an electronic data record or form moves from point to point with all of its data exposed, it is vulnerable to illegitimate exploitation each time it moves. Potential threats include identity theft, breach of privacy, theft or redirection of assets for illegitimate purposes, willful destruction or corruption of data, etc.

Moreover, when a business stores an entire electronic record or form, it incurs a legal obligation to maintain the confidentiality of any of the data that is sensitive in nature. By and large we have failed to tap the true potential of technology to reduce this exposure.

- Protection of data at rest¹
 - Unless data involved in a long-lived business transaction is protected and identified at each step of that transaction so that only the appropriate parties can access or update it, the data is at risk of being accessed or modified by unauthorized parties. Maintaining the records for certain financial transactions can be required for decades so that the long-term integrity of data at rest is important.
- Protection of data in transit²
 - Unless provisions are made for the protection and audit-ability of data in transit, involving security protocol interoperability, maintenance of digital signatures to record actions and events, etc., the data is at risk of being intercepted and compromised.
 - There exists a security risk in the unnecessary transmission and duplicate storage of sensitive data.
- Validity of data
 - Another key security issue is to minimize bad data getting into the system. Bad data may be kept for a long period of time, due to retention requirements, and be propagated throughout the system. Once such data is securely protected it may be even harder to remove.
- Distributed or federated repositories of data

¹ 'At rest' in this context means that the data is kept on a stable storage medium at one or more of the participants in the transaction, and possibly being processed by (an) application(s) that is (are) entirely local to these participants.

² 'In transit' in this context means that the data is being exchanged through electronic (or paper-based) means among two or more participants in a transaction.

- While the distribution and federation of data has the potential to render financial processes more efficient, it may also increase the risk of interception or compromise unless mechanisms are in place to properly authenticate identity in a cross-enterprise environment.
- Liability with respect to ownership of information
 - Unless security measures are robust or exercised with clear limits to indemnification, potential liability in authenticating identity and asserting authorizations across enterprises will slow the adoption of modern security mechanisms.
- Authentication and identification of stakeholders – Identity Management
 - Unless the referent of the data, i.e., the person or thing associated with the data, is uniquely and securely associated with data, accuracy and privacy of data are compromised.
 - There exists the possibility that participants in a transaction are not who they say they are and therefore should not be authorized.
 - Unless a mapping of the level of risk to the strength of the credential associated with a transaction is applied, risk-based acceptance of identity cannot be achieved, rendering the exchange of messages unduly expensive due to the risk value of the transaction.
- Cultural issues
 - From a global perspective, security issues can vary noticeably by region, and even within regions. For example, there exist regional variations (e.g. EU directives) on whose digital signatures can be accepted (e.g. that of employee of an enterprise vs. that of an enterprise as a whole) that the models need to take into account.

6.1.1.2 Potential Solution Strategies

What follows is a list of possible solutions to address the issues identified above. They are intended to seed the creation of next-generation models, where the financial processes are modified to be more efficient and secure.

- Minimize amount of information moved externally between Financial Services Institutions (FSI's):
 - Just-in time delivery of information, i.e., do not deliver it until it is needed.
- Use of non-contextual identifiers for various information sets:
 - Machine-generated identity systems will prevent any accidental or deliberate loss of referent information.

- Access rights should be associated within the context of these identifiers, and only for the necessary amount of time (note, however, that expiration of identifiers needs to be addressed carefully, as expiration may be undesirable, for instance for non-repudiation purposes or the need to keep information available for a longer period of time).
- Non-repudiation of sender and receiver
 - These mechanisms ensure that parties to a financial transaction cannot claim non-involvement.
- Consistent referencing (addressing) scheme for additional information
 - A consistent addressing scheme will allow the creation of indirect addressing mechanisms that will safely facilitate the reduction of information transmitted.
 - There is a requirement that references be resolvable for a long time after they have been created, possibly necessitating backward compatibility of algorithms and mechanisms.
- Introduction of third party Identity Management Services
 - These services will provide a mechanism for reduction of liability and can also protect participants from revealing competitive information.
 - Specific services to be offered are allocation, protection, and tracking of identity.
- Introduction of mutual authentication mechanisms
 - Some central authority is required (e.g. by Industry, by logical grouping of the participants in a payments infrastructure, etc.)
 - In some geographies, this is done through a governmental trust authority.
- Introduction of identity scoring technology, similar to credit score
- Introduction of a trust model where risk is evaluated against confidence and modified based on a financial service institution's familiarity with a customer vis-à-vis the value of the transaction
- Application of a layered approach to security, a common practice in the financial services industry, where risk is reduced by having layers within which security mechanisms work together.

6.1.2 Modeling Requirements necessitated by the security problems and solutions

The issues and potential solutions identified above can be framed through the judicious use of a set of models. In this RFP, the following types of model are identified.

- Data Model
 - An agreed upon and consistent data model and standard dictionary for funds transfer and account opening transactions is expected to underlie the process reference models.
 - This should include identification of primary or required data vs. supporting data.
 - Data characteristics should be distinguished, e.g., required, optional, etc.
- Service Model
 - The identification of the (ancillary) services that are required by the participants in a transaction to execute the transaction.
- Business Process Model
 - Effective, MOF-compliant models of the cross-enterprise business transactions involved in funds transfers and account openings.
 - Models of primary transactions and all secondary transactions, e.g., requests for identity, data reference look-up, etc., expressed as services defined in the Service Model.
- Trust Model
 - A model of the levels of trust required to conduct a transaction, dependent on the identity of the participants and the monetary amount of the transaction, and the mechanisms to implement and use such a trust model.
- Security Model
 - A model of the security requirements of the transaction as a whole as well as at each of the steps within the transaction; where appropriate, a layered approach to security as explained above should be applied.
 - The model should be aware that security should be designed to protect the access points, once the business process models are understood.

In addition, the following types of information need to be integrated in a comprehensive model:

- Description of timing requirements for each inter-enterprise transaction

- Length of time allowed for a transaction, length of time data must be held, etc.
- Description of all actors and roles potentially involved in transactions, both applications and personnel
 - Interface requirements of actors, including descriptions of the actions that the roles can take, as well as constraints and invariants associated with the actions.
 - Include regulatory actors and associated required information.
- Enumeration of Risk at various points in transaction
 - Utilize a consistent Risk function, including a measurement of liability.
 - Assess risk and liability trade-offs in a 'Business as Usual' context to the model.
 - Assess risk for unusual events, either accidental or deliberate.
- Description of header information required to support transactions
 - Identity codes, including unique message identification, transactions action path, etc.
 - Declaration of security protocols and mechanisms used.

The construction of models is further influenced by the following factors:

- Necessity to consider building local models or local variations to global models to account for regulatory differences across geographies.
- Necessity to consider cultural and national differences in the construction of the process models.

6.2 Scope of Proposals Sought

This RFP solicits proposals for a set of high level business process models to support the Financial Services Industry, specifically *account opening* and *funds transfer*. The models should address security and privacy of information.

The account opening and funds transfer processes were chosen because they are broadly applicable to the financial services industry, and they involve the transmission of sensitive data that usually crosses enterprise boundaries.

6.3 Relationship to Existing OMG Specifications

Proposed models should be expressed in (an) OMG modeling language(s).

Proposals should rely heavily on existing defined OMG standards, particularly UML, MOF, XMI, and business process modeling standards such as BPMN.

Submitters may consider using a SysML profile for financial services to add clarity to the models and facilitate requirements traceability.

6.4 Related Activities, Documents and Standards

Any new process modeling constructs derived can then be proposed to international standards organizations active in the financial services domain, such as the International Standards Organization (ISO) Technical Committee (TC) 68 through its Working Group (WG 4), which defines the ISO 20022 (UNIFI) standard for message-based financial transactions.

In addition, ISO TC 68 Subcommittee (SC) 2 (Security) has committed to evaluating the processes for accuracy and applicability.

The models will also be submitted to the FSTC for similar evaluation. Furthermore, the OMG and FSTC have agreed to provide a collaboration forum that all financial institutions and their suppliers, anywhere on earth, may join to help develop the response to this RFP

Proposals should reflect consultation and coordination with any emerging work to create financial service models that align with the UML 2.0 and MOF 2.0.

Models should leverage ongoing activity and existing modeling in the industry for account opening and funds transfers as well as the open standards work in this area, such as distributed process modeling, security modeling, identity management standards, etc.

The proposal should reflect awareness and compatibility with the major standards activities in the payments arena including ISO TC68 (Financial Services), the ISTH harmonization group, SWIFT standards activities, IFX standards committee, Visa International's standards activities, and others.

Of particular note in the payments industry is the PCI Data Security Standard (PCI DSS), whose requirements shall be taken into account in the responses to this RFP as well.

6.5 Mandatory Requirements

- 6.5.1 Proposals shall provide extensible models of funds transfer and account opening processes between financial institutions (as described in [6.1](#) and [6.2](#)) focusing on their applicability to the analysis of security issues (as described in [6.1.2](#)).
- 6.5.2 Models shall be expressed in a MOF-based modeling language, for instance the UML, where possible. Other OMG modeling languages, such as BPMN, may be used to augment MOF-based languages.
- 6.5.3 Proposals shall define an underlying data model in support of requirement [6.1.2](#).
- 6.5.4 Proposals shall define a UML-based service model in support of requirement [6.1.2](#), and capable of expressing the structure and use of ancillary services in a Service Oriented Architecture (SOA).
- 6.5.5 Proposals shall define a business process model in support of requirement [6.1.2](#).
- 6.5.6 Proposals shall define a trust model in support of requirement [6.1.2](#).
- 6.5.7 Proposal shall define a (layered) security model in support of requirement [6.1.2](#).
- 6.5.8 Proposed models shall provide full descriptions of actors and roles, including their interfaces.
- 6.5.9 The models shall be extensible.
- 6.5.10 Proposals shall define a MOF-compliant metamodel supporting the creation of models for other types of financial transactions.
- 6.5.11 Proposals shall define a UML profile for financial services processes to support the manipulation of the models in a UML tool.

6.6 Optional Requirements

- 6.6.1 Proposals may define funds transfer and account opening processes for:

- Corporate-to-Corporate transactions
- Corporate-to-Financial Institution transactions.

These should be extensions to or specializations of the corresponding processes defined earlier.

- 6.6.2 Submitters may apply a SysML profile for financial services to add clarity to the models and facilitate requirements traceability.

6.7 Issues to be discussed

- 6.7.1 Proposals shall discuss how an architectural framework based on the reference models can be used to identify opportunities for improved security and privacy mechanisms, protocols, and policies.

6.8 Evaluation Criteria

The proposals will be judged on the following criteria:

1. How well are these proposed reference models expected to be agreed on by the financial community?
2. How clearly and intuitively do the models provide a framework for communicating and exploring the security concepts identified?
3. How extensible are the models?
4. How effective and easy to use is the modeling methodology?
5. Is a MOF-compliant metamodel provided?
6. Is a UML profile provided?
7. Are the models comprehensive, i.e., are all the required models incorporated?
8. Is there a realistic approach to the assessment of trust, risk, and liability?

6.9 Other information unique to this RFP

None

6.10 RFP Timetable

The timetable for this RFP is given below. Note that the TF or its parent TC 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 at the *OMG Work In Progress* page at <http://www.omg.org/schedules/> under the item identified by the name of this RFP. Note that “<month>” and “<approximate month>” is the name of the month spelled out; e.g., January.

Event or Activity	Actual Date
<i>Preparation of RFP by TF</i>	
<i>RFP placed on OMG document server</i>	<i>March 5, 2007</i>
<i>Approval of RFP by Architecture Board</i>	

<i>Review by TC</i>	
<i>TC votes to issue RFP</i>	<i><approximate month></i>
<i>LOI to submit to RFP due</i>	<i><month> <day>, <year></i>
<i>Initial Submissions due and placed on OMG document server ("Three week rule")</i>	<i><month> <day>, <year></i>
<i>Voter registration closes</i>	<i><month> <day>, <year></i>
<i>Initial Submission presentations</i>	<i><month> <day>, <year></i>
<i>Preliminary evaluation by TF</i>	
<i>Revised Submissions due and placed on OMG document server ("Three week rule")</i>	<i><month> <day>, <year></i>
<i>Revised Submission presentations</i>	<i><month> <day>, <year></i>
<i>Final evaluation and selection by TF Recommendation to AB and TC</i>	
<i>Approval by Architecture Board Review by TC</i>	
<i>TC votes to recommend specification</i>	<i><approximate month></i>
<i>BoD votes to adopt specification</i>	<i><approximate month></i>

Appendix A References and Glossary Specific to this RFP

A.1 References Specific to this RFP

The following documents are referenced in this document:

[RFI] OMG RFI, "High Level Models of Financial Business Processes"
<http://www.omg.org/cgi-bin/doc?finance/2006-03-01>, issued by the FDTF

A.2 Glossary Specific to this RFP

None

Appendix B General Reference and Glossary

B.1 General References

The following documents are referenced in this document:

- [ATC] Air Traffic Control Specification,
http://www.omg.org/technology/documents/formal/air_traffic_control.htm
- [BCQ] OMG Board of Directors Business Committee Questionnaire,
<http://www.omg.org/cgi-bin/doc?bc/02-02-01>
- [CCM] CORBA Core Components Specification,
<http://www.omg.org/technology/documents/formal/components.htm>
- [CORBA] Common Object Request Broker Architecture (CORBA/IIOP),
http://www.omg.org/technology/documents/formal/corba_iiop.htm
- [CSIV2] [CORBA] Chapter 26
- [CWM] Common Warehouse Metamodel Specification,
<http://www.omg.org/technology/documents/formal/cwm.htm>
- [DAIS] Data Acquisition from Industrial Systems,
<http://www.omg.org/technology/documents/formal/dais.htm>
- [EDOC] UML Profile for EDOC Specification,
http://www.omg.org/techprocess/meetings/schedule/UML_Profile_for_EDO_C_FTF.html
- [EJB] “Enterprise JavaBeans™”, <http://java.sun.com/products/ejb/docs.html>
- [FORMS] “ISO PAS Compatible Submission Template”.
<http://www.omg.org/cgi-bin/doc?pas/2003-08-02>
- [GE] Gene Expression,
http://www.omg.org/technology/documents/formal/gene_expression.htm
- [GLS] General Ledger Specification ,
http://www.omg.org/technology/documents/formal/gen_ledger.htm
- [Guide] The OMG Hitchhiker's Guide,, <http://www.omg.org/cgi-bin/doc?hh>
- [IDL] ISO/IEC 14750 also see [CORBA] Chapter 3.
- [IDLC++] IDL to C++ Language Mapping,
<http://www.omg.org/technology/documents/formal/c++.htm>
- [MDAa] OMG Architecture Board, "Model Driven Architecture - A Technical Perspective", <http://www.omg.org/mda/papers.htm>
- [MDAb] “Developing in OMG's Model Driven Architecture (MDA),”
<http://www.omg.org/docs/omg/01-12-01.pdf>
- [MDAc] “MDA Guide” (<http://www.omg.org/docs/omg/03-06-01.pdf>)
- [MDAd] “MDA "The Architecture of Choice for a Changing World™””,
<http://www.omg.org/mda>
- [MOF] Meta Object Facility Specification,
<http://www.omg.org/technology/documents/formal/mof.htm>

- [MQS] “MQSeries Primer”,
<http://www.redbooks.ibm.com/redpapers/pdfs/redp0021.pdf>
- [NS] Naming Service,
http://www.omg.org/technology/documents/formal/naming_service.htm
- [OMA] “Object Management Architecture™”, <http://www.omg.org/oma/>
- [OTS] Transaction Service,
http://www.omg.org/technology/documents/formal/transaction_service.htm
- [P&P] Policies and Procedures of the OMG Technical Process,
<http://www.omg.org/cgi-bin/doc?pp>
- [PIDS] Personal Identification Service,
http://www.omg.org/technology/documents/formal/person_identification_service.htm
- [RAD] Resource Access Decision Facility,
http://www.omg.org/technology/documents/formal/resource_access_decision.htm
- [RFC2119] IETF Best Practices: Key words for use in RFCs to Indicate Requirement Levels, (<http://www.ietf.org/rfc/rfc2119.txt>).
- [RM-ODP] ISO/IEC 10746
- [SEC] CORBA Security Service,
http://www.omg.org/technology/documents/formal/security_service.htm
- [TOS] Trading Object Service,
http://www.omg.org/technology/documents/formal/trading_object_service.htm
- [UML] Unified Modeling Language Specification,
<http://www.omg.org/technology/documents/formal/uml.htm>
- [UMLC] UML Profile for CORBA,
http://www.omg.org/technology/documents/formal/profile_corba.htm
- [XMI] XML Metadata Interchange Specification,
<http://www.omg.org/technology/documents/formal/xmi.htm>
- [XML/Value] XML Value Type Specification,
<http://www.omg.org/technology/documents/formal/xmlvalue.htm>

B.2 General Glossary

Architecture Board (AB) - The OMG plenary that is responsible for ensuring the technical merit and MDA-compliance of RFPs and their submissions.

Board of Directors (BoD) - The OMG body that is responsible for adopting technology.

Common Object Request Broker Architecture (CORBA) - An OMG distributed computing platform specification that is independent of implementation languages.

Common Warehouse Metamodel (CWM) - An OMG specification for data repository integration.

CORBA Component Model (CCM) - An OMG specification for an implementation language independent distributed component model.

Interface Definition Language (IDL) - An OMG and ISO standard language for specifying interfaces and associated data structures.

Letter of Intent (LOI) - A letter submitted to the OMG BoD's Business Committee signed by an officer of an organization signifying its intent to respond to the RFP and confirming the organization's willingness to comply with OMG's terms and conditions, and commercial availability requirements.

Mapping - Specification of a mechanism for transforming the elements of a model conforming to a particular metamodel into elements of another model that conforms to another (possibly the same) metamodel.

Metadata - Data that represents models. For example, a UML model; a CORBA object model expressed in IDL; and a relational database schema expressed using CWM.

Metamodel - A model of models.

Meta Object Facility (MOF) - An OMG standard, closely related to UML, that enables metadata management and language definition.

Model - A formal specification of the function, structure and/or behavior of an application or system.

Model Driven Architecture (MDA) - An approach to IT system specification that separates the specification of functionality from the specification of the implementation of that functionality on a specific technology platform.

Normative – Provisions that one must conform to in order to claim compliance with the standard. (as opposed to non-normative or informative which is explanatory material that is included in order to assist in understanding the standard and does not contain any provisions that must be conformed to in order to claim compliance).

Normative Reference – References that contain provisions that one must conform to in order to claim compliance with the standard that contains said normative reference.

Platform - A set of subsystems/technologies that provide a coherent set of functionality through interfaces and specified usage patterns that any subsystem that depends on the platform can use without concern for the details of how the functionality provided by the platform is implemented.

Platform Independent Model (PIM) - A model of a subsystem that contains no information specific to the platform, or the technology that is used to realize it.

Platform Specific Model (PSM) - A model of a subsystem that includes information about the specific technology that is used in the realization of it on a specific platform, and hence possibly contains elements that are specific to the platform.

Request for Information (RFI) - A general request to industry, academia, and any other interested parties to submit information about a particular technology area to one of the OMG's Technology Committee subgroups.

Request for Proposal (RFP) - A document requesting OMG members to submit proposals to the OMG's Technology Committee. Such proposals must be received by a certain deadline and are evaluated by the issuing task force.

Task Force (TF) - The OMG Technology Committee subgroup responsible for issuing a RFP and evaluating submission(s).

Technology Committee (TC) - The body responsible for recommending technologies for adoption to the BoD. There are two TCs in OMG – *Platform TC* (PTC), that focuses on IT and modeling infrastructure related standards; and *Domain TC* (DTC), that focus on domain specific standards.

Unified Modeling Language (UML) - An OMG standard language for specifying the structure and behavior of systems. The standard defines an abstract syntax and a graphical concrete syntax.

UML Profile - A standardized set of extensions and constraints that tailors UML to particular use.

XML Metadata Interchange (XMI) - An OMG standard that facilitates interchange of models via XML documents.