

Object Management Group

140 Kendrick St
Building A, Suite 300
Needham, MA 02494

Telephone: +1-781-444-0404

Facsimile: +1-781-444-0320

High-Level Models of Business Processes for Financial Services

Request For Information

OMG Document: finance/2006-03-01

Responses due: June 2, 2006

1.0 Introduction

The Finance Domain Task Force of the Object Management Group seeks information from members of the financial services industry about inter-enterprise business processes that create, carry or consume sensitive data. Requested information will be evaluated by the OMG Finance Domain Task Force, resulting in the development of Requests for Proposal(s) (RFP) for standard reference models for a set of inter-enterprise business processes. These reference models are to be defined to elucidate the security issues across inter-enterprise, financial services networks. The financial services industry and their suppliers will then use these reference models to collaboratively define opportunities to improve security policy and controls.

The financial services industry has invested considerable resources to define standards, for security protocols, e.g., encryption using Public Key Infrastructure (PKI); for means of authenticating valid participants to financial processes; e.g., the work of the Extensible Authentication Protocol (EAP) committee; and for identity management, e.g., the Liberty Alliance Project. Though these activities are valuable to the financial industry; the protocols resulting from the work are functional solutions to particular security control and management problems. This RFI seeks a different approach from these protocols by addressing the security issues from the perspective of complete business activities that create, carry and consume sensitive data. The Task Force believes that standard reference models of business processes in financial services will provide a framework for properly and uniformly applying these existing functional protocols.

1.1 The Object Management Group (OMG)

With well-established standards covering software from design and development, through deployment and maintenance, and extending to evolution to future platforms, the Object Management Group (OMG) supports a full-lifecycle approach to enterprise integration which maximizes ROI, the key to successful IT. OMG's Modeling standards, the basis for the MDA, include the Unified Modeling Language (UML) and Common Warehouse Metamodel (CWM). CORBA, the Common Object Request Broker Architecture, is OMG's standard open platform with hundreds of millions of deployments running today. Headquartered in Needham, MA, USA, the Object Management Group is an international, open membership, not-for-profit computer industry specifications consortium. More information about OMG can be found at www.omg.org.

1.2 **OMG Finance Domain Task Force**

The Finance Domain Task Force of the Object Management Group (OMG), a global standards organization, requests information of the financial industry about common business processes that create, carry or consume sensitive data. This

Task Force expects to use the information to build new standard reference models of Business Processes in Financial Services. The standard reference model will enable application engineers, system architects, and information security engineers to clearly identify where security vulnerabilities exist in inter-enterprise financial information communications and to begin the dialogue on how to address these vulnerabilities.

1.3 RFI Objectives

1.3.1 What is an OMG RFI?

The intent of an OMG Request for Information (RFI) is to gather information for guiding a subgroup in its efforts to provide solutions to industry problems. The RFI process is used by a subgroup to canvass a targeted industry segment for one or more of the following purposes:

- Acquiring general or specific information about industry requirements.
- Soliciting assistance in identifying potential technology sources.
- Soliciting input to validate a subgroup's roadmap.

Generally speaking, the RFI process determines which Request For Proposals (RFPs) will be issued (and, based on negative feedback, which won't) or influences the way a particular RFP is constructed.

2.0 Information Being Requested

2.1 Summary of this RFI

Unauthorized access or use of sensitive customer information concerns all financial institutions. The proliferation of personally identifiable, private information has had unintended consequences for organizations including inappropriate release of sensitive data. For example, a third party contractor improperly handled unencrypted information, exposing millions of private records.

The risk of unauthorized access has increased. The distribution mechanisms and channels that handle financial transactions have expanded greatly with the advent of the Internet and the World Wide Web. These new distribution channels use business processes that span multiple enterprises. Although positive results are achieved, these channels have increased security exposures; e.g., improper identity verification can increase liability for exposing sensitive data; or improper access authorization can allow multiple fraudulent transactions. The solution to these security problems requires new community standards because no single enterprise can implement cross-enterprise solutions. To address these more global business concerns, the financial industry should collaborate to develop uniform industry standards to protect sensitive data. (Note: The Financial

Domain Task Force expects that, once developed, these same standard reference models will prove useful for solving similar internal security problems within an enterprise.)

This Request for Information seeks responses from members of the financial services industry. The information desired includes definitions of sensitive data, including variations across political jurisdictions, and the methods now employed for the data's creation, transport, storage and consumption across organizational boundaries. The Task Force expects to use this information to establish standard reference models of key financial processes, particularly those that concern personally identifiable, sensitive data. The Task Force expects to construct models of key business processes to allow the members of the financial industry to better understand potential security risks and vulnerabilities, and communicate this information, as technical requirements, clearly and unambiguously, to information security system engineers.

The purpose of the RFI also is to understand means currently used in the industry for communicating vulnerability information to security teams. The manner in which the reference models are presented should be useful to security engineers who are then better able to protect sensitive information; e.g., develop standard diagrams that may be consumed by security engineering teams.

To begin creation of standard reference models, respondents should provide answers to these questions relative to specific business processes: "How is sensitive data defined? What are the flows of this information? With whom and in what manner is it exchanged? For what purpose is it exchanged? How is it generated? Where is it kept and how is it used? What sensitive data is minimally required to complete a financial process?"

Respondents also should answer questions about typical security protocols that apply to cross-enterprise, business processes. These include: "What protection and controls are applied? What kinds of data encryption are utilized? How is identity information managed? How are security policies and contractual obligations tracked and enforced? How are they audited? What assurance means are provided to maintain the integrity, interoperability, maintainability, availability, recoverability and reliability of an institutions' security policies?"

Two processes have been identified as potential candidates for reference modeling: **account opening** and **payments**. These processes were chosen because they are broadly applicable to the industry, and they involve sensitive data that usually crosses enterprise boundaries. This RFI also seeks responses supporting or negating this hypothesis.

This RFI also requests information that includes data and anecdotes about vulnerabilities, current processes, controls and technologies in relation to the business processes described in the respondent's submission. It also requests proposed solutions and improvements that have or could reduce vulnerabilities in the processes. For example, improvements may reduce information transmission requirements or standardize controls and protections for sensitive consumer

information. Responders also are asked to identify means whereby these standard reference models may be produced and consumed.

2.2 Detail

Respondents are asked to respond to as many of the questions listed below as they are able. A future meeting of the Finance Domain Task Force will be scheduled at which respondents will be able to present and discuss their answers and provide additional clarifying information and examples to their peers.

- 2.2.1 **What are the flows of sensitive data?** The flows of interest are those that occur between enterprises. It is not necessary to give elaborate details about such flows at this time. Enough information should be supplied in order that a general flow diagram can be created; for instance: an account opening process requires a prospective customer to enter personally identifiable, private information into a web browser screen supported by a third party outsource firm, information is then sent through file transfer to an FI, etc.
- 2.2.2 **What is the purpose of the exchange?** Respondents should provide a high-level description of one or more business processes that create, consume or carry information across organizational boundaries. These business processes should be clearly explained. The Task Force has suggested two processes that are good candidates for reference modeling: “*account opening*” and “*payments*”.
- 2.2.3 **With whom and in what manner is such information exchanged?** The information sought here is at a high level of description and is related to the business processes request described in 2.2.2. The response should include an abbreviated discussion of the nature and location of the trading partners.
- 2.2.4 **How is the information generated; where is it kept, for approximately how long; and how is it used?** The answers to these questions must relate the business processes described 2.2.2 and 2.2.3. However, such information provided should be at a high level of description.
- 2.2.5 **What minimal sensitive data is required to complete a business process?** The information requested here seeks to understand the necessary and sufficient conditions for the business processes and data flows identified in 2.2.2, 2.2.3 and 2.2.4 to complete successfully. It may be useful to express rationale for accepting more information than is minimally required to complete these processes.
- 2.2.6 **How is identity information managed?** Sensitive data usually involves personal identities, customer lists, security controls and the like. The respondent should only consider identities that are involved in the business processes identified in 2.2.2.
- 2.2.7 **What security measures typically are applied to the suggested business processes, including standard protections and controls?** Here the

respondents only should provide information that is ***not confidential*** and at a very high level of description. Preferably the response will use industry standard terms in the answer. How are policies and contractual obligations tracked and enforced?

2.2.8 **What assurance means are provided to maintain the integrity, interoperability, maintainability, availability, recoverability and reliability of the institutions' security measures?** The information provided should be non-confidential and at a very high level of description. Anecdotes about vulnerabilities in the financial networks, current processes, controls and technologies would be helpful.

2.2.9 **How should reference models be presented?** The purpose of the RFI also is to understand the means for communicating the information to security teams. Hence, respondents also are asked to identify means whereby these standard reference models may be produced and consumed.

2.3 Discussion of the proposed process

2.3.1 Review of the Larger Problem

The geometric increase in connectivity and the proliferation in exchanges of personally identifiable private information, brought about by the telecom and Internet revolutions have significantly changed the security landscape. As new distribution and connectivity technology is introduced, new risks have been introduced and the old standby situations have become riskier. For example, the ability to execute transactions remotely over the Internet make the possession of sensitive personal information, relied on to identify and authenticate individuals, more valuable, as they can be used to commit fraud faster, less expensively, and with less risk of getting caught. Collectors amass and sell sensitive personal information collected with common tools or through insider data theft; this data is then used to actually commit fraud, such as fraudulent transfer of money, fraudulent purchase of goods, and fraudulent opening of accounts under false identity. Accidental, inappropriate release of sensitive data also occurs, with the unintended consequence of creating substantial liability for the organizational owners of that data.

The problem space of focus for this RFI is on the risks associated with the requirement for and misapplication of sensitive, customer information that is involved inter-enterprise business transactions. The scope of concerns is around both the transport and storage of such data. Customers can be both persons as well as corporate entities.

2.3.2 Value of Standard Reference Models

The Finance Domain Task Force anticipates that the production of standard reference models for key financial processes; i.e., those requiring creation, transport, consumption and storage of sensitive data; would be followed by standards that would reduce risks of misuse of sensitive data.

For example:

1. Reduce amount of information that is transmitted e.g., by clearly associating information required for a particular process and not requiring non-essential information.
2. Reduce copies of information within the network as a whole by removing obstacles to real-time information sharing e.g., anonymous request and replies, lowered liability associated with supplying information, surrogated information, etc.
3. Reduce vulnerabilities by identifying and prescribing corrections for those vulnerabilities such as encrypting data and access audits, etc.

For these or other standards to take hold, industry agreement on enriched inter-enterprise security standards and processes will be required. The need for agreed upon standards and processes as the focus is on the inter-enterprise space where no one enterprise can dictate a solution is clear.

2.3.3 The First Step – Creating Reference Models

The first step in promoting this discussion and analysis is to define common reference models for some key cross-enterprise processes, since none of this work can begin without common reference models that frame that analysis and discussion.

This RFI is specifically focused on gathering information about that first step; by identifying qualified banking-based business transactions that should be modeled; second by identifying available content and methodology that can be utilized to produce these reference models.

Two transactions – Account Opening and Payments -- have been selected as clearly involving the cross-enterprise transport of sensitive customer information and having universal relevance. The RFI welcomes suggestions for other transactions that will yield a reference model with the right framework for security analysis.

Account opening was chosen as in almost all cases sensitive customer information is transmitted. It can be sent over the Internet as entered by the customers themselves, transmitted from another financial institution, sent from a third party service. In any case account openings result in risky transmittal of information as well as the risky redundant storing of that data in many sites. The process is a target for committing fraud (e.g. opening a fraudulent account using someone else's identity).

Payments were chosen as the direct risks associated with these transactions are high since the effect of a payment transaction is a transfer of funds.

This RFI expects to gather existing information, anecdotes, and especially modeling work associated with these transactions. In addition the RFI solicits an overview of security concerns and solutions associated with these transactions. Finally, responses to the RFI should elucidate the industry organizations,

corporations and service providers that are actively involved in related, relevant modeling and/or security initiatives.

2.3.4 Discussion of reference models

The purpose of these reference models is to provide a framework for discussions and analysis of security issues. The methodology for creating the reference models must be clear, to a great extent self-documenting. The models are expected to reside in widely available, easily used modeling tools. Also the resulting models must include a consistent and widely acceptable ontology, both for the elements in the models as well as the transactions operators.

This RFI solicits information sources, experiences and analysis of the modeling methodology and tools that would be most appropriate. Discussions of trade-offs among alternatives will be especially useful.

2.3.5 Practical goals and objectives for modeling effort

It is important in the work that results from the RFI that “we don’t bite-off more than we can chew”. This RFI solicits information, analysis, and opinion on the appropriate scope for the reference models. Responses should provide insight into trade-offs and pitfalls that should be considered. They should also frame the proposed modeling effort within the scope of existing activities of other groups. One key goal of the RFI is that existing work is properly leveraged and our work adds significant but focused value to creating the chosen reference models.

2.4 Process and Participation

2.4.1 Schedule for RFI

Step 1: (2/15/2006) Refined RFI based on feedback, to be presented at OMG Tampa Technical Session

Step 2: (last week of 3/2006) RFI Workshop to focus responses

Step 3: Presentations of responses to the RFI (4/26/2006)

Step 4: Develop draft RFP based on RFI submissions at OMG Anaheim Technical Session (09/25-29/2006.)

Step 5: (12/2006) RFP published.

2.4.2 Respondent Working Session

All respondents have the opportunity to present their responses to this RFI at a future meeting of the Finance Domain Task Force. Arrangements can be made to give these reports in person at the meeting or by teleconference. Respondents are urged to remember, information submitted to the Finance Domain Task Force, as response to the RFI, is public information. Caution should be exercised to keep the information in the response generic to the finance industry as your organization participates in it.

3.0 Instructions for Responding to this RFI

The Financial industry currently operates under significant burdens of liability for inappropriate or inadvertent disclosure of personally identifiable, private information. These disclosures may be purely accidental or criminally fraudulent. Without a common model of how, what, when, why and where sensitive data is shared, organizations can only undertake error prone, exhaustive research into sources of potential sources and uses of sensitive data.

- 3.1.1 The respondents will have an opportunity to learn from their peers about business processes that share sensitive data, sometimes without the consent or knowledge of the recipient. Due to the long legacy of using financial networks, previously thought to be “private”, information remains in old formats that may not be required for any legitimate business processes. Without a standard model of what the industry understands common business processes to be, and what information is required for their function, liability exposure and maintenance costs may remain unnecessarily high.

All members of the financial services industry, information security and information technology suppliers are invited to respond to the RFI.

4.0 Instructions for Responding to this RFI

4.1 Who May Respond

Responses from anyone in industry, government or academia with practical knowledge of inter-enterprise business processes in financial services and the security and privacy issues associated with those business processes are welcome to respond to this request for information.

When and if OMG issues a subsequent Request for Proposal(s) (RFP) in this area, OMG members at the appropriate membership level will be eligible to respond with detailed proposed specifications. OMG is an open membership organization. Any company, university or organization is welcome to join and participate. For information, consult <http://www.omg.org/membership>.

4.2 How to Respond

One electronic copy in machine-readable format (typically ASCII, MS Word, or WordPerfect format) should be sent to ***omg-documents@omg.org***. One confirming paper copy of all documents should be sent to the OMG postal address below.

Object Management Group, Inc.

140 Kendrick St.

Building A Suite 300

Needham, MA 02494

USA

Attn: **High-Level Models of Business Processes for Financial Services RFI**

Responses to this RFI must be received at OMG no later than 5:00 PM US Eastern Time (22:00 GMT) June 2, 2006

Other communication regarding this RFI should be sent to the contacts listed in paragraph 4.8.

4.3 RFI Response Contact

Companies responding to this RFI shall designate a single contact within that company for receipt of all subsequent information regarding this RFI and the forthcoming series of RFPs. The name of this contact will be made available to all OMG members.

4.4 Format of RFI Responses

The following outline is offered to assist in the development of your response. You should include:

- A cover letter -- the cover letter should include a brief summary of your response, such as indicating to which areas you are responding and must also indicate if supporting documentation is included in your response.
- The response itself, covering any or all of the areas of information requested by this RFI.
- If required, a glossary that maps terminology used in your response to OMG standard terminology. (See OMG specifications [CORBA, UML, MOF, XMI] and a description of OMG's Model Driven Architecture [MDA] for OMG's standard terminology.)

Although the OMG does not limit the size of responses, you are asked to consider that the OMG will rely upon volunteer resources with limited time availability to review these responses. In order to assure that your response receives the attention it deserves, you are asked to consider limiting the size of your response (not counting any supporting documentation) to approximately 25 pages. If you consider supporting documentation to be necessary, please indicate which portions of the supporting documentation are relevant to this RFI.

4.5 Distribution of RFI Responses

Copies of all documentation submitted in response to this RFI will be available to all OMG members for review purposes.

4.6 Copyrighted Material

According to OMG Policies and Procedures, proprietary and confidential material shall not be included in any response to the OMG. Any material received is treated as a public document. If copyrighted material is sent in response to this RFI then a statement waiving that copyright for use by the OMG

is required and a limited waiver of copyright that allows OMG members to make up to twenty-five (25) copies for review purposes is required. Consult Appendix B for a template for this copyright waiver.

4.7 Reimbursement

The OMG will not reimburse submitters for any costs in conjunction with their responses to this RFI.

4.8 Questions Regarding this RFI

Any technical questions regarding this RFI should be sent to:

Mark Eisner	or	Joe Bugajski
FireStar Software		Visa International
eisner@firestarsoftware.com		JBugajski@visa.com

Questions regarding the response process should be forwarded to:

Object Management Group, Inc.
140 Kendrick St
Building A Suite 300
Needham, MA 02494
USA

Attn: Mr. Juergen Boldt, Director of Member Services

Phone: +1-781-444 0404

Fax: +1-781-444 0320

Email: juergen@omg.org

5.0 Response Review Process and Schedule

5.1 Review Process

OMG RFIs are issued with the intent to survey industry to obtain information that provides guidance, which will be used in the preparation of RFPs. The OMG membership, specifically the OMG Finance Domain Task Force, will review responses to this RFI. Based on those responses, the OMG Finance Domain Task Force will augment its roadmap and prepare one or more RFPs.

5.2 Clarification

To fully comprehend the information contained within a response to this RFI, the reviewing group may seek further clarification on that response. This clarification may be requested in the form of brief verbal communication by telephone; written communication; electronic communication; or a presentation of the response to a meeting of the OMG Finance Domain Task Force.

5.3 RFI Response Presentations and Demonstrations

RFI Respondents may be invited to present their response to the OMG Finance Domain Task Force. The purpose of this presentation would be to seek clarification of information contained within the response (as noted above); to further explore issues raised; or to further meet the goals of the RFI.

In addition, a technology demonstration to the OMG Finance Domain Task Force may prove useful to support the RFI response. If desired, please coordinate with the Contact cited in paragraph 4.8.

5.4 Schedule

The schedule for responding to this RFI is as follows. Please note that early responses are encouraged.

RFI responses due:	June 2, 2006
Review of RFI responses:	June 26, 2006
Release of first RFP:	December 8, 2006

Appendix A References and Glossary Specific to this RFI

A.1 References Specific to this RFI

[CORBA] http://www.omg.org/technology/documents/formal/corba_iiop.htm.

[MDA] MDA Technical Perspective, <http://doc.omg.org/ab/2001-02-01>.

[MOF] Meta-Object Facility (MOF),
<http://www.omg.org/technology/documents/formal/mof.htm>.

[UML] Unified Modeling Language (UML),
http://www.omg.org/technology/documents/formal/unified_modeling_language.htm.

[XMI] XML Metadata Interchange (XMI),
http://www.omg.org/technology/documents/formal/xml_metadata_interchange.htm.

Appendix B Template for Copyright Waiver for RFI Responses

[Date]

Object Management Group, Inc.
140 Kendrick St
Building A, Suite 300
Needham, MA 02494
Attn: James Nemiah, General Counsel

Fax: 781-444-0320

Dear Mr. Nemiah:

This letter constitutes a limited license to use certain materials copyrighted by the undersigned. We understand that the Object Management Group, Inc. (“OMG”) is a not-for-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications.

We understand that the Copyrighted Material identified below is being submitted to OMG as part of a response to the identified Request for Information (RFI), for use in connection with an OMG process that may result in the adoption of an OMG specification.

Source of Copyrighted
Material:

Copyrighted Material to be
submitted to OMG:

Submitter(s):

RFI Doc.-Title & No.

We hereby grant OMG the right to make an unlimited number of copies of the Copyrighted Material as part of the OMG adoption process.

We hereby grant each OMG member the limited right to make up to twenty-five (25) copies of the Copyrighted Material for review purposes only as part of the OMG adoption process.

Regards,