


INTERNET ARCHIVE
WayBackMachine
BETA

[11 captures](#)
6 May 02 - 21 Sep 05



SEP MAY SEP
2002 2003 2004
22

[Close](#)
[Help](#)

Operating Rules

*For use in the Electronic Procurement Project
Known as the "Multi-State E-Mall"™*

Version 2.0

The Current Version of this Document is Available at:
<http://email.isa.us/or>

COPYRIGHT NOTICE

Copyright © 1999 by the Commonwealth of Massachusetts. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts, as Policy Authority for the Multi-State EMail; and (2) all copies must include this notice of copyright.

Table of Contents

[A. Scope](#)

[A.1. General](#)

[A.2. Application of these Operating Rules](#)

[A.3. Open Buying on the Internet](#)

[A.4. Contact Information](#)

[B. Authentication: In General](#)

[B.1. Issuance, Use, Modification and Termination of User Name and Passwords](#)

[B.2. Use of SSL](#)

[B.3. Use of S/MIME](#)

[B.4. Use of Fax, Telephone, U.S. Mail, Commercial Couriers, and Unsecured/Unauthenticated E-Mail](#)

[C. Authentication: Certificate Policy](#)

[C.1. Introduction](#)

[C.2. General Provisions](#)

[C.3. Identification and Authentication](#)

[C.4. Operational Requirements](#)

[C.5. Physical, Procedural, and Personnel Security Controls](#)

[C.6. Technical Security Controls](#)

[C.7. Certificate and CRL Profiles](#)

[C.8. Specification Administration](#)

[D. Roles, Functions and Authorization of Participating Parties](#)

[D.1. General Concepts](#)

[D.2. Role: Policy Authority \(EMail Team/Principal\)](#)

[D.3. Role: Business Administrator \(EMail Team/Admin.\)](#)

[D.4. Role: Operations Administrator \(EMail Team/Admin.\)](#)

[D.5. Role: State Partner MOU Signatory \(State Partner/Principal\)](#)

[D.6. Role: State Coordinator \(State Partner/Contact\)](#)

[D.7. Role: Shopper \(State Partner/User\)](#)

[D.8. Role: Operational Approver \(State Partner/User\)](#)

[D.9. Role: Financial Approver \(State Partner/User\)](#)

[D.10. Role: Receiver \(State Partner/User\)](#)

[D.11. Role: Supplier Partner MOU Signatory \(Supplier Partner/Principal\)](#)

[D.12. Role: Supplier Coordinator \(Supplier Partner/Contact\)](#)

[D.13. Role: Certificate Manufacturer](#)

[D.14. Role: Solution Providers](#)

[E. Technical Requirements](#)

[E.1. User Personal Computer](#)

[E.2. Supplier Partner](#)

[E.3. Physical Security of Computing and Network Resources](#)

[F. Duties and Obligations of the Parties](#)

[F.1. Creation of Legally Binding Purchases](#)

[F.2. Notice](#)

[F.3. Participation Agreements](#)

[F.4. Confidentiality](#)

[F.5. Intellectual Property](#)

[F.6. Alternative Dispute Resolution](#)

[F.7. Governing Law](#)

A. Scope

A.1 General

The Multi-State Email pilot (Email) is an Extranet procurement Web site, hosted by the Commonwealth of Massachusetts and available to participating states (known as State Partners in this document). The Email web site provides links to qualified Supplier "storefronts" or catalogs, where state procurement staff (known as authorized State Users) can browse, shop and create requisitions. Public Key Certificate technology coupled with user name and password ensure that only authorized State Users can submit approved OBI Orders to the approved suppliers (known as authorized Supplier Partners). In addition, casual, non-privileged Internet users can access certain public portions of the site, but can not engage in binding transactions unless they are authorized participants in this pilot and agree to accept these Operating Rules.

A.2 Application of these Operating Rules

These Operating Rules apply to every participant in the Email. No party may play any role or otherwise act as a participant in the Email without signing a Participation Agreement. Depending on the role a given party plays (i.e. User, Supplier, Administrator, etc.) a different Participation Agreement with special terms may be required.

A.3 Open Buying on the Internet

The Email is based upon the Open Buying on the Internet (OBI) specification. OBI is an emerging standard that defines the technical requirements for conducting business over the Internet from buyer to seller. The following definition is copied from the OBI web site:

The OBI standard is an open, flexible design for business-to-business Internet commerce solutions. It is intended for the high-volume, low-dollar transactions that account for 80% of most organizations' purchasing activities. Version 1.0 of the standard document contains an architecture, as well as technical specifications and guidelines. OBI is not a product or a service; it is a freely available standard which any organization can obtain and use.

Information about the OBI standard is available at the web site <http://www.openbuy.org>. Version 1.0 and Version 1.1 of the OBI technical specifications are available from this site.

A.4 Contact Information

The Policy Authority promulgating these Operating Rules is the Commonwealth of Massachusetts. A current version of these Operating Rules and related information is available at <http://email.isa.us>. Signed Participation Agreements of each party performing a role under these Operating Rules are on file with the Policy Authority.

For purposes of business communications, parties performing a role in the EMall may contact:

Nancy Burke, EMall Project Manager,
Commonwealth of Massachusetts, Operational Services Division
One Ashburton Place, Room 1017
Boston, MA 02108
nancy.burke@osd.state.ma.us, 617.720.3187

For questions or comments specifically relating to these Operating Rules, parties performing a role in the EMall may contact:

Daniel Greenwood, Deputy General Counsel, Information Technology Division & EMall Counsel and Steering Committee Member
Commonwealth of Massachusetts
One Ashburton Place, Room 801
Boston, MA 02108

dan.greenwood@state.ma.us, or dan@civics.com, 617.973.0071

B. Authentication: In General

B.1. Issuance, Use, Modification and Termination of User Name and Passwords

A User name and Password must be supplied by every User of the EMall Server accessing a non-public portion of the system. No User may share or otherwise reveal their Password or other authorized Personal

Identification Number (PIN). Any suspicion that a Password has been compromised must be immediately communicated to the State Coordinator for that User. A Password may be re-set in the event that an authorized User forgets the Password. A User should contact their State Coordinator, who can authorize a password reset from the Operations Administrator. Upon proper notification by an authorized State Coordinator under these Operating Rules and relevant implementing agreements, a User's access to the EMall will be terminated and the respective User name and Password combination for a terminated User will no longer be valid.

In addition to transmission of the valid Public Key Certificate, User identification for access to the EMall server also requires presentation of a user name that corresponds with the Common Name of the Subscriber as listed in the Public Key Certificate (and that is unique within the EMall User profiles) and must be transmitted with the corresponding valid password or PIN.

B.2. Use of SSL

Every person accessing any non-public portion of the EMall server must use the Secure Sockets Layer (SSL) protocol. The SSL protocol will be used to authenticate and secure certain communications between Supplier servers and the EMall server as well as to encrypt certain session between the browser of a User and the EMall server and authenticate the identity of authorized EMall Users. A web session invoking version 3 of the SSL protocol requires use of a duly issued Public Key Certificate within the browser of an EMall User. SSL 3 is also required to authenticate and secure the transmission of a valid OBI Order from the EMall server to the server of a Supplier.

B.3. Use of S/MIME

A Pilot Participant who is duly issued a Public Key Certificate for use in the EMall may use that Public Key Certificate to "sign" e-mail to another participant. In addition, a Pilot Participant may use the duly issued EMall Public Key Certificate of another participant to encrypt e-mail using the S/MIME standard, provided each person uses an interoperable e-mail client. In some cases, as determined by an EMall Administrator, use of S/MIME may be requested or required to assure official communications via e-mail are confidential and/or authenticatable.

B.4. Use of Fax, Telephone, U.S. Mail, Commercial Couriers, and Unsecured/Unauthenticated E-Mail

B.4.1. General

Access as a User or Administrator to the EMall server will require a valid User name and Password as well as a recognized Public Key Certificate. However, many other communications channels will be used for various other purposes throughout the term of this pilot. It is recognized that implementation of a production system will require greater specificity regarding permitted and prohibited methods of communication and corresponding authentication depending on the purposes of the communications. It is intended that

experience gained through this pilot process will demonstrate appropriate guidelines. For purposes of the pilot, however, it is expected that most non-critical communications will occur between pilot participants via phone and e-mail.

B.4.2. Communication of Agreements and Related Data

Communication of the implementing agreements under these Operating Rules and related User designation and authorization data requires greater specificity. Until and unless otherwise specified in future versions of these Operating Rules, delivery of all completed forms, agreements and related data, including all designation of roles and authorities for Users of the EMail system must be communicated via:

- * Fax, U.S. Mail or Commercial Couriers, or

- * Upon prior approval by the EMail Business Coordinator, S/MIME Signed E-Mail, signed by private key corresponding to a validly issued Public Key Certificate for the EMail pilot

Until and unless return receipt is received by phone call back or other agreed methods, sender must consider that such data has not been successfully transmitted.

B.4.3. Other Communications

Unless otherwise specified in these Operating Rules, communications may be conducted by any reasonable means that are appropriate under the circumstances..

C. Authentication: Certificate Policy

C.1. Introduction

For purposes of the Multi-State EMail pilot, a Public Key Certificate (Certificate) is a computer-based record which:

- (a) identifies the entity or brand associated with issuance of it;
- (b) names or identifies the person or device associated with the corresponding private key;
- (c) contains the public key corresponding to that private key of that person or device; and
- (d) is digitally signed by the Certificate Manufacturer that creates the Certificate.

In transacting business over the Internet, it is critical that both the seller and buyer be assured that the transactions exchanged are secure. Public key encryption coupled with Public Key Certificates can provide part of this security by ensuring the confidentiality and/or authentication of electronic business exchanges. When Public Key Certificates are attached to transactions, parties on each side of a purchase have some evidence of who the message came from and that it was not tampered with. The EMall pilot uses Certificates to bolster the authentication provided by the Password and User name in the EMall system. A Certificate is not, by itself, sufficient to perform any transactions within the EMall system.

Public Key Certificates are used to authenticate Web servers and their clients via protocols such as SSL 3.0. A Public Key Certificate is analogous to an identification card issued by an employer or membership organization. Each User participating in the EMall pilot must have at least one Public Key Certificate. Certificates will be issued at no cost by a designated and contracted party known as a Certificate Manufacturer (CM). The CM will issue a Certificate to Users who have been identified by their respective State Coordinators and accepted by the EMall Administrator.

The browser specifications, as noted in the Section E Technical Requirements, accommodates the use of Public Key Certificates. A technical resource for each State Partner will be needed to assist each User with the installation of that User's Certificate. This technical resource and/or the state coordinator must have an adequate understanding of the technical and operational requirements and responsibilities associated with managing, issuing and maintaining Public Key Certificates. The technician shall not have knowledge of any User's password.

This Certificate Policy section of these Operating Rules governs creation, delivery and other aspects of the Certificate Manufacturing process as well as the proper use of Public Key Certificates. This section follows the format of the Internet Engineering Task Force PKIX Part 4 Framework (available at <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt>) and is in general accord with the guidance provided by Version 1.0 of the draft "Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates" by the Certificate Authority Ratings and Trust (CARAT) Task Force of the Internet Council of the National Automated Clearinghouse Association (NACHA) available at <http://internetcouncil.nacha.org/CARAT/> . Please note that many of the basic business and legal terms surrounding each party's role within the EMall are properly addressed in other sections of these Operating Rules and will either supplement or replace information reserved under IETF PKIX-4 headings (such as "liability" and "financial responsibility" etc.).

C.2. General Provisions

C.2.1 Obligations

C.2.1.1 Policy Authority Obligations

The Policy Authority pays for most or all of the EMall pilot and has initiated the effort to create this pilot.

The chief obligation of the Policy Authority is to sponsor and organize the EMail pilot, to set policy, including this certificate policy, and to assure the smooth and successful operation of the pilot. The policies are set in a manner that affords input and comment from State Partners and other Pilot Participants.

C.2.1.2 PKI Service Providers

C.2.1.2.1 Registrars

The Registrar, is the sole point of contact between the PA and the CM for purposes of requesting the issuance of certificates. The Registrar is ordinarily the EMail Business Administrator. However, when necessary, the EMail Operations Administrator may act as Registrar. The Registrar must keep records of each application request and valid certificates issued. Each State Coordinator shall also act as a Local Registrar for purposes of designating authorized Users and therefore certificate subscribers.

C.2.1.2.2 Operations Administrators

The Operations Administrator (OA) sets the EMail server to grant access authorized subscribers based on the unique information in each subscriber's certificate. The OA is responsible for acquiring and installing "commercial off the shelf" server certificates on the main EMail server as well as training and development servers, as needed. In addition, the Operations Administrator is responsible for installing the CM's root certificate on each EMail server that will process subscriber certificates and for the distribution of root certificates to each authorized Supplier that will act as a Relying Party.

C.2.1.2.3 Certificate Manufacturers

The Certificate Manufacturer (CM) only has duties and responsibilities toward the Policy Authority and duly designated Administrators and not directly toward any other pilot participant, other than as specified in this section of the Operating Rules or as agreed upon by and between the CM, the PA and each such other party. The CM shall manufacture Public Key Certificates according to the certificate profile contained in this Certificate Policy upon the request of the Registrar. Each such certificate shall reflect accurately the information contained in the certificate application, including the Common Name and the State associated with each applicant.

C.2.1.3 End Entities (Parties or Their Devices that Use or Rely Upon Certificates)

C.2.1.3.1 Subscribers

C.2.1.3.1.1 Users

Each EMall User (including Shoppers, Approvers and Receivers) shall be issued a Public Key Certificate upon designation and authorization by their respective State Coordinator and successfully completing and submitting their User Agreement. A User's EMall certificate does not represent a generic identification or authorization credential for use outside the EMall. A User is obligated to refrain from using their EMall certificate in any communications with non-EMall Pilot Participants or for non-EMall related business. A User must provide accurate information in the User Agreement and related forms and to their respective State Coordinator with respect to EMall activities. A User must immediately notify their State Coordinator upon notice or reasonable suspicion that information within their certificate is no longer accurate, including upon the termination of their employment. A User must immediately notify their State Coordinator upon notice or reasonable suspicion that the private key corresponding to their certificate has been compromised (see User Documentation and User Agreement for more information). A User must abide by the terms and conditions of their User Agreement.

C.2.1.3.1.2 EMall Server Certificate for User Sessions

The EMall server and such other training or support servers as are designated by the EMall Operations Administrator shall have installed a valid Server Certificate. To be valid, under this section, a Server Certificate must be signed by a CM whose certificate signing key is recognized (without further customization) by each Browser that is supported for use within the EMall (see Section E. of these Operating Rules). That means that the public key that corresponds to the private key used to sign the Server Certificate must be embedded within each such browser at the time the Browser software is distributed and requires no further installation of a root certificate or other prefatory work in order to invoke an SSL session. In addition, a valid certificate must be used only within the starting and ending dates designated in the Server Certificate and must be replaced prior to expiration of said ending date.

C.2.1.3.1.3 EMall Transaction Server Certificate for OBI Order Transmissions

The EMall Server Transaction Certificate shall be a public key certificate used to initialize an encrypted http session and to identify the EMall server to authorized Supplier transaction server for the purpose of sending Valid OBI orders using SSL 3. The Operations Administrator shall assure that a valid EMall Server Transaction Certificate is installed on the EMall server and will make sufficient information about the contents of that certificate known to each authorized Supplier who will act as a Relying Party upon that certificate.

C.2.1.3.1.4 Other Pilot Participants

For purposes of testing, support and other activities approved by the PA or authorized Administrator, any other EMall Pilot Participant may be issued a Public Key Certificate. Where an individual other than a User issued a certificate, that person must first agree to abide by relevant sections of these Operating Rules and any other terms and conditions deemed appropriate by the PA or it's authorized Administrator. These

additional terms must, at a minimum, specify the purpose and authorized uses of the certificate within the EMail pilot.

C.2.1.3.2 Relying Parties

C.2.1.3.2.1 Administrators

The Operations Administrator must require and accept valid EMail certificates as part of the initial authentication of authorized Users of the EMail server. Use of a certificate alone shall not be sufficient proof of identity for purposes of gaining access to User-only section of the EMail server, but must be accompanied by the authentication requirements specified in Part B. of these Operating Rules.

C.2.1.3.2.2 Suppliers

Suppliers may rely upon valid EMail certificates to identify and authenticate a subscriber as an authorized Shopper, as that role is defined under these Operating Rules. Suppliers must rely upon a certificate to authenticate and secure valid OBI Orders from the EMail server. Suppliers may rely upon certificates to identify a subscriber via S/MIME signed e-mail, but may not assume any authorization based solely upon usage of a certificate used for this purpose. Suppliers may not rely upon EMail certificates for any other purposes than those specified in these Operating Rules.

C.2.1.3.2.2.1 Shopper Browser Certificate Used for Authentication to Supplier Web Catalog

A Supplier should, but need not utilize a subscriber certificate of a Shopper for authentication. A Supplier that does not rely upon the subscriber certificate for authentication directly may rely upon certificate and other User authentication performed by the EMail server and securely passed on to the Supplier at the beginning of a web catalog session for purposes of shopping. A Supplier that uses a subscriber certificate for purposes of authentication must, at a minimum:

- * assure that the certificate was manufactured by the authorized CM for the EMail, based upon the root certificate distributed by the Operations Administrator; and
- * identify the State of the Shopper from within the certificate for purposes of assuring the correct contracted items and prices are displayed and that the correct OBI Order Request information is transmitted.

C.2.1.3.2.2.2 EMail Server Transaction Certificate for OBI Orders Used for Authentication to Supplier Transaction Server

The EMail Server Transaction Certificate shall be a public key certificate used to identify the EMail server to authorized Supplier transaction server for the purpose of sending Valid OBI orders. All Suppliers must utilize a secure and authenticated SSL 3 (dual authenticated) session for the transmission of valid OBI Orders from the EMail server. If the SSL 3 session necessary to commence transmission of an OBI Order to a Supplier transaction server is invoked without a Public Key Certificate or via a Public Key Certificate other than that provided for under section C.2.1.3.1.3 of these Operating Rules (EMail Server Transaction Certificate), then the resulting transaction must be regarded as invalid. The risk that an unauthorized OBI Order could be generated that conforms with the format, content and other process constraints comprising a valid EMail OBI Order is extremely low, but the risk does exist. If a Supplier wishes to further minimize this risk, then the Supplier should configure their transaction server to accept EMail OBI Orders only from the pre-authorized EMail Server Transaction Certificate, based upon certificate information provided to the Supplier by the EMail Operations Administrator under section C.2.1.3.1.3.

C.2.1.3.2.3 Pilot Participants

No Pilot Participant may use their certificate to authenticate themselves to any person or device outside of the EMail pilot. All Pilot Participants can use their Public Key Certificates to send signed e-mail to any other Pilot Participant. In addition, any Pilot Participant may use the Public Key Certificate of another pilot participant to send encrypted e-mail to that person. Not all Pilot Participants are necessarily entitled to an EMail certificates.

C.2.2 Liability

Liability is not dealt with in the Certificate Policy, rather it is governed by the underlying business contracts and other relevant business agreements between parties participating in this pilot. This Certificate Policy exists for the purpose of further defining and clarifying details of this authentication method and does not comprise the business relationship between the parties.

C.2.5 Fees

Certificates are provided at no cost to Pilot Participants.

C.2.6 Publication and Repository

The CM maintains a non-public, web-accessible repository of valid and revoked certificates. For security purposes no further information on this repository is available in these Operating Rules. From time to time the PA or it's designated Administrators may request access to this repository according to terms and processes as mutually agreed between the PA and the CM.

C.2.7 Compliance Audit

No Compliance Audit is necessary under these Operating Rules. More detailed duties and obligations between the PA and the CM can be found in the Implementing Contract between those parties by which the CM is contracted to provide certificate manufacturing services.

C.2.8 Confidentiality

See section F.4 of these Operating Rules.

C.2.9 Intellectual Property Rights

See section F.5 of these Operating Rules.

C.3. Identification and Authentication

The process and practices governing identification and authentication of subscribers are determined by the EMail Business Administrator, with the knowledge and assent of the EMail Steering Committee and the agreement of each State Partner Coordinator. The Business Administrator may customize these processes and practices to conform to different management and organizational environments among the various State Partners and other authorized Subscribers. Material procedures must be documented and available for review by the EMail Steering Committee and any other party with a business need or legal right of access to that information. Documented processes and relevant practices may be changed throughout the pilot, but any material changes must require the knowledge and consent of the EMail Steering Committee.

C.4. Operational Requirements

See Section C.2 of these Operating Guidelines for relevant Operational Requirements.

C.5. Physical, Procedural, and Personnel Security Controls

The CM, PA and relevant Administrators shall agree upon appropriate physical, procedural and personnel security controls, as needed.

C.6. Technical Security Controls

The CM, PA and relevant Administrators shall agree upon appropriate technical security controls, as needed.

C.7. Certificate and CRL Profiles

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes. The syntax and semantics underlying the EMall Certificate Profile is available, to the extent necessary, upon request from any authorized Relying Party who needs the information to accept or process Public Key Certificates and to conform to relevant Risk Management guidelines, as provided under these Operating Rules and by the Policy Authority.

C.8. Specification Administration

The Policy Authority is the Specification Administration. Matters such as publication, notice of change and rights to comment on rules changes are dealt with throughout these Operating Rules and are not unique or specific to the use of any one authentication method for this business system. The use of public key certificates, and the policies related to such use, is part of the overall business system underlying the EMall pilot. General issues related to Notice of change of these Operating Rules, including any changes to the Certificate Policy sections of these Operating Rules, can be found in Section F.2.

D. Roles, Functions and Authorization of Participating Parties

D.1. General Concepts

Party: A legal entity. A natural person can be a party. Certain organizations, such as corporations, trusts and governments may also be recognized as a legal person and therefore can be a party. Each party will be identified by name in relevant documents and agreements. Actions of an automated program, including an electronic agent, are deemed to be the actions of a party that used the program for that purpose, under these Operating Rules.

Functions: The particular duties and obligations entered into within a business and technical system. A Party will perform several functions. These sets of functions are put together based on technical, legal and business needs of the enterprise.

Role: Each *role* is named according to the nature of the functions in each set. By naming roles, and associating functions with roles, it is not suggested that in every business model sets of functions will be divided in the same manner as here. Further, it is not suggested that there will be one-to-one correlation between roles and parties. Indeed, it is envisioned that a *party* may perform one or more roles. The purpose for naming roles in this document is primarily to provide a vocabulary for creating modular parts that can be perform by a given party entering the EMall system and to organize the obligations and related documents associated with a given party.

For example, rather than call the administration role by the name Commonwealth of Massachusetts, it is convenient to name it based on the relevant suite of functions so that any party could perform the role more easily within the system of documents and business arrangements herein. Similarly, while particular parties perform the role of service providers, there may be additional and/or different parties playing those roles in the future, hence we use terms like "solution provider" and "Certificate Manufacturer." The usage of roles under these Operating Rules is intended to reflect and support the potential evolution of this project from a relatively closed and small pilot to a scalable production system in which many more parties may perform the roles noted herein.

Documents and Agreements: In many cases, a party will have to sign a document or submit a particular form as part of the functions associated with a given role. These documents might be contracts, memoranda of understanding, applications, reports and so on. These documents hold a particular legal importance as the glue that hold together parties, roles and functions in a predictable and enforceable system.

Pilot Participants: Every party that agrees to be bound by the Operating Rules is considered to be a "Pilot Participant." This general designation defines the closed community of people who are part of the EMall pilot. All of the parties whose roles are described below (not limited to Users alone) are also considered Pilot Participants because they all agree to be bound by these Operating Rules and to operate within the pilot in some authorized manner.

D.2. Role: Policy Authority (EMall Team/Principal)

Functions

- * Sponsor of the Multi-State EMall pilot;
- * Makes all policy decisions related to the Multi-State EMall pilot;
- * Designates, and delegates appropriate authority to EMall Administrators;
- * Agrees to accept the MOU of State Partners; and
- * Selects and arranges for technology products and services necessary for hosting the EMall OBI-Compliant server on behalf of State Partners as buying organizations.

Relevant Documents and Agreements

- * Promulgates, or delegates authority to promulgate, these **Operating Rules** and all other official agreements or documents related to the Multi-State EMall.

D.3. Role: Business Administrator (EMall Team/Admin.)

Functions

- * Receives names/contact data of each State Coordinator from each designated Partner State (from person(s) who signed the MOU);
- * Gives the State Coordinator contact information to the Operations Administrator;
- * Reviews and submits for processing all security related applications and forms, including those related to Public Key Certificates, which are forwarded by the State Coordinator; and
- * Securely maintains all applications and forms for related Public Key Certificate requests before and after processing by the EMail Operations Administrator.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Must sign **Business Administrator Agreement**.

D.4. Role: Operations Administrator (EMail Team/Admin.)

Functions

- * Responsible for administering the EMail servers, including the IEC Server and the Database Server;
- * Responsible for creating and/or amending and/or terminating User accounts and related User authorizations on EMail system in accordance with instructions from EMail Business Administrator; and
- * Responsible for accurately ascertaining the identity of an authorized User prior to performing a password reset. Calling the purported User back at the pre-authorized telephone number designated by that User's State Coordinator is a reasonable basis for confirming the identity of an EMail User.
- * Responsible for requesting Certificate Manufacturer to create and deliver a Public Key Certificate to each authorized User.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Must sign **Operations Administrator Agreement** governing authorization rights and responsibilities to the EMail Server and related matters.

D.5. Role: State Partner MOU Signatory (State Partner/Principal)

Functions

- * Agrees to be an EMail Pilot Participant by signing the State MOU;

- * Designates the authorized Coordinator for the participating State Partner; and
- * Sponsors a Supplier for participation in the EMail with a valid, current contract with that state.

Relevant Documents and Agreements

- * Signs the **State MOU** that includes reference to agreement with policy materials (herein known as these **Operating Rules**).

D.6. Role: State Coordinator (State Partner/Contact)

Functions

- * Primary Operations and Business point of contact for communications with EMail Administrators;
- * Designates state Users and their respective authorization rights, including designation as a Shopper, Approver, or Receiver;
- * Assists User in application process and with use of the EMail system;
- * Designates authorized Supplier Partner(s); and
- * Immediately notifies the EMail Operations Administrator of changes in authority (including termination) for any User or Supplier.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules. Signs State Coordinator Agreement and User Designation and Authorization** forms for each authorized User.

D.7. Role: Shopper (State Partner/User)

NOTE: The role of Shopper is also known as "Requisitioner" for certain technical purposes within the I.E. C. application and the EMail system.

Functions

- * May shop on and through the EMail system;
- * May act, with the prior permission of the EMail Operations Administrator, as a User of the EMail system through the use of an Electronic Agent, as defined under the most current draft or applicable enacted Uniform State Law, including Article 2 of the Uniform Commercial Code, draft proposed Article 2B and the draft proposed Uniform Electronic Transactions Act [links to official current drafts and related information is available at: <http://www.state.ma.us/itd/legal/agents>];

- * Must use system only for authorized purposes and not use Public Key Certificate for any non-EMall pilot purpose;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Shopper will:
 - * shop available EMall catalogs on the Web to determine best value;
 - * select a participating Supplier;
 - * access the Supplier's storefront (electronic catalog) with contracted pricing in the EMall;
 - * select items to be purchased;
 - * create an OBI Order Request with the Supplier;
 - * verify in-house inventory availability as appropriate;
 - * adjust the OBI order request as necessary; and
 - * complete the OBI Order, flagging the OBI Order for operational approval.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.8. Role: Operational Approver (State Partner/User)

Functions

- * May shop and must process approved OBI Orders created by other Shoppers;
- * May act, with the prior permission of the EMall Operations Administrator, as a User of the EMall system through the use of an Electronic Agent, as defined under the most current draft or applicable enacted Uniform State Law, including Article 2 of the Uniform Commercial Code, draft proposed Article 2B and the draft proposed Uniform Electronic Transactions Act [links to official current drafts and related information is available at: <http://www.state.ma.us/itd/legal/agents>];
- * No Approver may approve an OBI Order that they placed themselves unless they have been specifically authorized by the appropriate personnel at their state and that authorization has been successfully communicated to the EMall Administrator by the Approver's Sate Coordinator (note: this exception will be approved in appropriate circumstances, such as when a User works in a one person departments);
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Operational Approver will:
 - * review the OBI Order Request;
 - * adjust the OBI Order Request as necessary; and

- * approve or deny the OBI Order Request on-line, flagging the OBI Order for Financial Approval.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.9. Role: Financial Approver (State Partner/User)

Functions

- * May shop and must verify that the appropriate "encumbrance" and payment related financial controls for their state have been satisfied and documented;
- * May act, with the prior permission of the EMall Operations Administrator, as a User of the EMall system through the use of an Electronic Agent, as defined under the most current draft or applicable enacted Uniform State Law, including Article 2 of the Uniform Commercial Code, draft proposed Article 2B and the draft proposed Uniform Electronic Transactions Act [links to official current drafts and related information is available at: <http://www.state.ma.us/itd/legal/agents>]
- * This role may be combined with the Operational Approver;
- * Must enter relevant "legacy system" encumbrance and payment related numbers into the EMall system;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, and /or the legacy accounting system as appropriate, the Financial Approver will:
 - * verify funds availability;
 - * process an encumbrance in the legacy accounting system known as: legacy system;
 - * cross-reference the legacy system encumbrance and OBI Order Request for audit purposes and release the detailed OBI Order for EDI 850 Transmission;
 - * review and adjust invoices submitted for payment electronically in the EDI 810 format through the EMall;
 - * process payment in the legacy accounting system known as: legacy system;
 - * update payment information on the OBI Order;
 - * financial approval must ensure that an appropriate legacy system entry has been made before an OBI Order is sent to the Supplier.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.10. Role: Receiver (State Partner/User)

Functions

- * Must indicate in the system when commodities shipped as a result of an EMail OBI Order have been received in full and/or part, making notations as appropriate concerning the exceptions noted at the time of delivery;
- * Must document exceptions within the EMail system and any necessary legacy system;
- * May act, with the prior permission of the EMail Operations Administrator, as a User of the EMail system through the use of an Electronic Agent, as defined under the most current draft or applicable enacted Uniform State Law, including Article 2 of the Uniform Commercial Code, draft proposed Article 2B and the draft proposed Uniform Electronic Transactions Act [links to official current drafts is available at: <http://www.law.upenn.edu/library/ulc/ulc.htm>) and additional non-binding, but helpful information can be found at: <http://www.tiac.net/biz/danielg/agents/>];
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Receiver will:
 - * accept and verify commodities received;
 - * record receipt of commodities in the EMail.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.11. Role: Supplier Partner MOU Signatory (Supplier Partner/Principal)

Functions

- * Makes catalogs available according to the OBI specification as implemented for EMail through the EMail Operating Rules;
- * Is an authorized Supplier for purposes of doing business with the EMail Partner state that sponsored that Supplier and with such other participating EMail Partner States as agreed by the parties;
- * Accepts the EMail transactional system (including the various usages of authorized Public Key Certificates) and their own authorized transaction server as a valid and binding method of transmitting quotes and receiving orders (also known as OBI Order Requests and OBI Orders, respectively), as specified under these Operating Rules;
- * Designates Supplier Coordinator.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **Supplier MOU** and the **Electronic Commerce Supplier Partner Agreement**.
- * Signed respective **contracts** with the sponsoring state pursuant to applicable procurements laws for purposes of doing business with that state.

D.12. Role: Supplier Coordinator (Supplier Partner/Contact)

Functions

- * Primary Operations and Business point of contact for EMail communications with the Supplier Partner;
- * Responsible for responding to delivery or payment inquiries and disputes, including by use of the query function, as available, within the EMail system.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.

D.13. Role: Certificate Manufacturer

Functions

- * Creates Public Key Certificates as requested by EMail Operations Administrator;
- * Creates said Certificates according to the Certificate profile specified by EMail Policy Authority;
- * Abides by the Certificate Policy section of these Operating Rules.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**, including **Section C. Authentication Certificate Policy** (Certificate Policy), and warrants that any internal documented practices, such as a Certificate Practice Statement, are consistent with these Operating Rules and the included Certificate Policy.
- * Signs **Certificate Manufacturer Agreement**.

D.14. Role: Solution Providers

Functions

- * Provide products and services necessary for State Partners to conduct OBI-Compliant transactions via the EMail;

- * Conduct initial system set up and testing;
- * Upon agreement and request, provide ongoing support to the EMall Operations Administrator as contracted and/or on a time and materials basis.

Relevant Documents and Agreements

- * Agrees to abide by the **Operating Rules**.
 - * Signs contract and agrees to Task Order with Policy Authority for provision of services and related products.
-

E. Technical Requirements

For this pilot, the State User Department agrees to comply with the technical standards which are detailed below:

E.1. User Personal Computer:

The minimum computer requirements and configuration is detailed below:

E.1.1. Internet and World Wide Web Connectivity

A computer capable of accessing the World Wide Web (WWW), which implies connectivity to the Internet using the TCP/IP protocol.

E.1.2. Hardware:

- Pentium Processor
- 32MB memory
- 10 MB of available disk space on the hard drive
- 10/100 Ethernet network interface card
- A mouse
- Year 2000 compliant
- Monitor: 17 inch or greater SVGA monitor, with a minimum of 800X600 pixels of resolution
- ADA compliant

E.1.3. Software:

- Windows 95 or Windows NT 4.0 Workstation

- A 4.0 or higher version of the Netscape Navigator or Internet Explorer browser to allow the use of Secure Sockets Layer (SSL) 3.0
- A Public Key Certificate to be installed within the User's browser and used to authenticate the identity of a User will be issued by the Certificate Manufacturer contracted to provide services to the EMall
- Year 2000 compliant.
- ADA compliant

Comparable hardware and software is acceptable but resolution of problems arising from their use is the sole responsibility of the User's department.

E.2. Supplier Partner

Every party that agrees to perform the role of a Supplier Partner must, at a minimum, provide a web-based catalog that is compliant with the OBI 1.1 specification, as referenced under these Operating Rules.

E.3. Physical Security of Computing and Network Resources

The EMall Web Server must be kept in a physically secure location such that unauthorized persons can not gain physical access to the server without breaking and entering. There are no physical security requirements for Users during the course of the pilot, however, no User may permit an unauthorized person to gain access to a computer that is currently accessing a restricted area of the EMall server (that is, once a User logs onto the system with a user name, password and Public Key Certificate, that User should not leave their computer accessible to any other person until logging off the EMall server). There are no physical security requirements for Suppliers during the course of the pilot. The Certificate Manufacturer must assure that no unauthorized personnel may gain physical access to the private key for the root Certificate for this pilot or may otherwise become capable of manufacturing unauthorized Public Key Certificates.

F. Duties and Obligations of the Parties

F.1. Creation of Legally Binding Purchases

A valid OBI Order must be generated as the result of the authorized approval process specified in Section D of these Operating Rules. Every valid and enforceable sale of goods through the EMall pilot resulting from an OBI Order shall be subject primarily to the underlying contracts between the relevant Supplier and State User and also shall be subject to these Operating Rules and related agreements as well as the terms

and conditions within the OBI Order itself. In order to be merged into the final terms of a purchase, any provisions inserted into an OBI Order Request must conform to the OBI Specification as implemented within the EMail pilot. The terms ***OBI Order Request*** and ***OBI Order*** are to be construed in accordance with the OBI 1.1 specification, as referenced in these Operating Rules. For purposes of this section, the term ***EMail Server*** shall mean the web server hosted on behalf of the State Partners for the purpose of conducting OBI-compliant transactions and shall include the EMail Transaction Server referenced in Section C of these Operating Rules. For purposes of this section, the term ***Supplier Server*** shall mean the web server of a Supplier Partner for the purpose of conducting OBI-compliant transactions, including the Supplier Transaction Server referenced in Section C. of these Operating Rules.

F.1.1. OBI Order Request

An OBI Order Request shall constitute a contractual offer by the Supplier Partner to sell the specified commodities at the specified price and other included terms once it has been successfully posted by the Shopper's web browser to the EMail Server at the agreed upon post-back URL.

F.1.2. OBI Order

An OBI Order shall constitute a contractual acceptance by the transacting State Partner once it has been successfully posted by the EMail Server to the Supplier Server at the agreed upon post-back URL.

F.2. Notice

Every party that has been authorized as a participant after having signed and delivered a participation agreement for the EMail pilot is entitled to notice of any proposed amendment to these Operating Rules at least 14 calendar days prior to said amendments taking effect, unless otherwise agreed by all the parties. In the case of a State Partner, the person(s) who sign the State MOU and each authorized State Coordinator are entitled to receive notice and may be requested or required to pass along such notice to each subordinate User within their state if appropriate. Notice may be communicated via e-mail, fax or other reasonable means, however, unless notice is delivered via U.S. Postal Mail, the Policy Authority must confirm that each party so entitled has in fact received notice. An e-mailed reply confirming receipt by a party to the Policy Authority is a valid means to confirm delivery of notice to that party.

F.3. Participation Agreements

As noted under these Operating Rules, a party that performs an authorized role within the EMail must sign an agreement, known generally as a Participation Agreement. A key function of each Participation Agreement is to signify the assent of each party to abide by these Operating Rules. Parties who will assume a role within the EMail pilot may retrieve a current version of their respective agreements in PDF form from the official EMail web site. These agreements must be completed, signed, and returned to the EMail Business Administrator in order for any person to become an authorized EMail Pilot Participant.

F.4. Confidentiality

Unless otherwise specified in these Operating Rules and related agreements and to the extent permitted under applicable law, all personally identifiable information related to the EMall pilot, including User information, usage statistics related to an individual User, the names of administrators, any telephone, address or other individually identifiable data should be considered confidential and should not be disclosed to any person outside of the EMall pilot. Similarly, no Pilot Participant should make any public statements including press releases, information available on a web site and slide presentation related to the EMall pilot or about any other person or organization's participation in the EMall pilot, unless that statement has first:

- * appeared on the official EMall web site, or
- * appeared in the public press, or
- * been authorized by an EMall Administrator, or
- * is a matter of public record under applicable law

F.5. Intellectual Property

These Operating Rules are subject to Copyright by the Commonwealth of Massachusetts in its capacity as sponsor of the Multi-State EMall. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts in its capacity as Policy Authority for and sponsor of the Multi-State EMall; and (2) all copies must include this notice of copyright.

"Multi-State EMall" is a trademark of the Commonwealth of Massachusetts.

F.6. Alternative Dispute Resolution

Disputes between a State User and a Supplier regarding the purchase of goods, including pricing, quality or service guarantees and remedies, shall be governed according to the terms and conditions contained within the underlying contract for the purchase of goods as between those parties. Disputes arising out of or related to the application of these Operating Rules and related Participation Agreements shall be resolved in accordance with the provisions of these Operating Rules and related agreements, and by agreement between the parties, where possible, through direct negotiation or, if appropriate, through voluntary mediation by a mutually agreed upon Mediator.

Depending upon the nature and gravity of a given dispute, as well as the geographic distance of the parties, use of Online Alternative Dispute services may be appropriate. Such services include the Virtual Magistrate program (<http://vmag.vcilp.org/>) and, generally, the services referred to in the Massachusetts Information Technology Division's background paper on Online ADR (<http://www.state.ma.us/>

[itd/legal/adr.htm](#)). Use of Online Alternative Resolution services is explicitly permitted under these Operating Rules, if otherwise agreed upon by all the parties. In the event that parties are unable to reach agreement directly or through the use of mediation or other voluntary methods of Alternative Dispute Resolution, then, to the extent permitted by law and relevant regulation, all such disputes shall be subject to binding arbitration by a mutually agreed upon arbitrator of the American Arbitration Association. The costs of any form of Alternative Dispute Resolution shall be paid equally by the disputants or as otherwise agreed by the parties.

F.7. Governing Law

Disputes between a State User and a Supplier regarding the purchase of goods, including pricing, quality or service guarantees and remedies, shall be governed according to the law of jurisdiction so noted in the underlying contract for the purchase of goods between those parties, or, if no such jurisdiction is so noted, then it shall be deemed to be the laws of the state of the User. Disputes arising out of or related to the application of these Operating Rules and related Participation Agreements shall be governed according to the law of the Commonwealth of Massachusetts.