

COMMONWEALTH OF VIRGINIA



Information Technology Resource Management Standard

MIDDLEWARE STANDARD

Department of Technology Planning

Preface

Publication Designation

COV ITRM Standard MID2001-01.1

Subject

Middleware

Effective Date

December 7, 2001

Supersedes

No prior middleware standards

Scheduled DTP Review

One (1) year from effective date

Authority

Code of Virginia, § 2.2-226
(Powers and Duties of the Secretary of Technology)

Code of Virginia, § 2.2-2651
(Powers and Duties of the Council on Technology Services)

Code of Virginia, § 2.2-1701
(Powers and Duties of the Department of Technology Planning)

Scope

This standard is applicable to all state agencies and institutions of higher education (hereinafter collectively referred to as "agencies") that are responsible for supporting certain types of applications including for example, e-mail services, which must communicate across the network within an N-tier environment. This standard is offered as guidance only to local government entities.

Purpose

The setting of standards for information technology architecture components is done to comply with laws, which, in part, have been passed to encourage greater efficiencies and effectiveness in the use of technology to accomplish government business. The standards are to inform agency staff of opportunities for better meeting strategic and tactical information technology development objectives. In the case of middleware, the opportunities lie in providing vehicles for reducing costs, improving security, improving reliability, improving communications, and adding functionality. Middleware can enhance interagency cooperative efforts, agency to business cooperative efforts, intra-agency n-tier program-to-program

communications, and application functionality. This document identifies middleware functions and/or tools that may enable greater efficiencies and effectiveness if implemented centrally within an agency, or in a standard way across agencies.

Objectives

To explain the interplay of industry-supported standards, Virginia laws, Governor's Executive Orders, and sound enterprise business practices in providing an architectural foundation for the cost-effective development of applications that are dependent upon middleware functions and tools and that are needed to conduct the business of Virginia's agencies.

To provide agencies with Virginia's requirements related to middleware infrastructure development, maintenance and administration.

General Responsibilities

In accordance with the *Code of Virginia*, the following provisions apply:

Secretary of Technology

Responsible for:

- Directing the formulation and promulgation of policies, standards, specifications, and guidelines for information technology in the Commonwealth, including, but not limited to, those (i) required to support state and local government exchange, acquisition, storage, use, sharing, and distribution of geographic or base map data and related technologies and (ii) concerning the development of electronic transactions including the use of electronic signatures as provided in § [59.1-496](#).
- Directing the establishment of statewide standards for the efficient exchange of electronic information and technology, including infrastructure, between the public and private sectors in the Commonwealth.

Council on Technology Services (COTS)

Responsible for :

- Advising and assisting the Secretary of Technology in exercising the powers and performing the duties conferred.

Department of Technology Planning (DTP)

databases (e.g., Oracle), or specially written programs (e.g., programs using XML).

Responsible for:

Assisting the Secretary of Technology in the development of statewide policies affecting technology at all levels of government, in the business sector, and among the general citizenry.

- Developing and promulgating policies, standards, and guidelines for managing information technology in the Commonwealth.
- Developing statewide standards for the efficient exchange of electronic information and technology, including infrastructure, between the public and private sectors in the Commonwealth.

All State Agencies

Responsible for:

- Cooperating with the Secretary of Technology, the Department of Information Technology, and the Department of Technology Planning in the performance of their powers and duties.
- Complying with the Department of Technology Planning's policies, standards, and guidelines for information technology resources in the Commonwealth.

Definitions

Middleware is most often software and in some cases, hardware, which may perform many integral functions in a networked environment and which may provide sets of useful tools for applications that run in a networked environment. In an N-tier environment, applications may communicate with databases, other applications, users, etc. to accomplish their work. This requires messaging between players. Middleware addresses both messaging and tools that help to ensure the ongoing reliability of both simple communications and more complex, multi-step transactions. Middleware is not one thing. Middleware tool sets are often called by names including database middleware, transaction-processing middleware, messaging middleware, remote procedure call middleware, etc. Middleware may function within a LAN environment or over the Internet. Middleware has been described as the "glue" that ties applications together. Middleware functions may be provided by operating systems (e.g., Windows 2000), separate software bundles (e.g., middleware by Candle or Software AG),

Related COV ITRM Policies, Standards, and Guidelines

COV ITRM Policy 95-1, Statewide Implementation of Electronic Commerce, dated August 8, 1995, addresses the Electronic Data Interchange (EDI) standard for electronic commerce. EDI may be classified as an international standard related to middleware functions. The ITRM policy document that addresses e-commerce and EDI will be reissued as a middleware policy upon further investigation of electronic commerce trends. Electronic commerce methods are rapidly changing to include options other than EDI.

Table of Contents

Background.....	1
Approach.....	1
Reviews.....	1
Statement of ITRM Requirements for Middleware.....	2
Resources.....	6
Requesting Waivers to Requirements.....	8
Glossary.....	10
Appendix A: Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines.....	11

Background

Earlier Commonwealth ITRM policies, standards and guidelines did not specifically address middleware. The term, middleware, is relatively new in the definition of computing architectures. Separate middleware products have mushroomed in recent years along with the growth of multi-tiered applications, e-business, and multi-platform, distributed computing environments. As agencies of the Commonwealth increase the number of networked applications they support, they must also increase their attention to standardizing their computing architectures with respect to those “middle” functions common across their networked applications.

Middleware provides vehicles for enabling agencies to move from stovepipe application architectures to more integrated systems. Among the services and tools provided by middleware are centralized and distributed directory services and robust enterprise-wide messaging services.

This document addresses the standardization of selected middleware functions and tools across state agencies and universities (referenced herein as agencies). This standardization is expected to benefit both individual agencies and groups of agencies working on common networked computing efforts. The requirements presented emanate from the work of the Enterprise Architecture Middleware Domain team. The team had state agency, local government, and higher education members.

Approach

This document will provide: 1) a listing of the middleware related requirements adopted by the Commonwealth, 2) reference materials and Web sites related to the requirements, and 3) a general discussion of how state agencies would typically address the requirements.

Any standards from the Internet Engineering Task Force (IETF) and other standards bodies referenced as requirements within this document are adopted in both their present state and as amended or replaced unless otherwise indicated in the statement of Information Technology Resource Management (ITRM) requirements provided below.

Every effort will be made to ensure that requirements in this document are reviewed annually. Whenever standards bodies introduce major modifications, this will trigger a midyear review of requirements by the Department of Technology Planning. As reviews are conducted, the review dates and recommended modifications will be added to this document.

Reviews

Revisions anticipated within the next 12 months are mainly the movement of various IETF standards (e.g., LDAP versions) from proposed standards to draft standards to

Internet standards. A full review of the COV ITRM Standard MID2001-1.1 is anticipated one year from the release date.

Statement of ITRM Requirements for Middleware

The following ITRM requirements for state agencies address common middle functions that may serve to increase opportunities for more cost-effective computing across applications both within agencies and across agencies of the Commonwealth. Standardization with respect to these middle functions provides an architectural foundation that is important for conducting the future business of the Commonwealth. For a comprehensive overview of middleware architecture for the Commonwealth, please see the *Middleware Architecture Report* at: [http://www.sotech.state.va.us/cots/ea/documents/Middleware_Architecture - Approved.doc](http://www.sotech.state.va.us/cots/ea/documents/Middleware_Architecture_-_Approved.doc).

Requirement 1. Directories Accessible by LDAP.

State Agencies must deploy network directories that may be accessed using the Lightweight Directory Access Protocol (LDAP). The purpose of this requirement is to ensure broad future accessibility to the mission-critical information that is contained in directories regardless of which agencies are building the directories or whether the directories are centralized or distributed.

LDAP is a vendor neutral protocol. Directories of most major platforms claim LDAP compliance (e.g., Active Directory, NDS, SDS, etc.).

A directory may be described as a specialized database of lists. Directories serve a wide variety of functions in a computing environment and are used by applications including email, security, and naming services. Directory services are important as tools in the communications process and decisions about directory services are one of the most important foundation decisions an agency can make in planning a distributed architecture and middleware strategy. Deciding on a desired external directory strategy (e.g., external to the database system or network management system) before looking at middleware products will allow an agency to be more critical of how middleware components are integrated, especially in bundled, multi-vendor products. Having a directory strategy is an integral part of promoting interoperability, location transparency, and lower future maintenance costs in a distributed environment. Some directory services can be configured with strong security by attribute so that everyone may see a user e-mail address for example but only the user could update a password or see other personal information. Some example uses of a directory to support government functions are provided below:

- Certificate authority information and public keys for digital signatures;
- Single sign-on password information for employees and other authorized individuals;

- A statewide citizen-changeable address store that could be accessed by subscribing agencies;
- Encrypted agency PIN numbers for citizen access to services;
- Object naming for reuse by programmers; and
- Employee address, office phone or email information for updating by employees.

Directories are powerful tools within networked computing environments. Ensuring access to directories is often mission critical. Directory providers must work with network administrators to ensure that:

- sensitive directory information is protected by appropriate authentication and access restrictions;
- the network design has addressed potential security threats including denial of services and man in the middle attacks; and
- the passing of private information to or from directories is done with appropriate encryption.

One underlying requirement for protocols in the LDAP suite is that they work with X.500 directories; however, the Commonwealth is not requiring that its agencies develop X.500 directories. This ITRM Middleware Standard focuses entirely on access to directories. How directories are developed is only important in that the directory structure may have an impact on accessibility.

The relationship between LDAP access and X.500 protocols is that LDAP has incorporated a subset of the functions provided in the X.500 directory access protocol, DAP. LDAP was developed as an alternative to DAP. DAP was viewed as too complex and its interface was based on the Open Systems Interconnect or OSI seven layer model of network computing rather than the less complex TCP/IP model (Transmission Control Protocol/Internet Protocol). TCP/IP is today's *defacto* inter-networking standard and is also Virginia's Networking Enterprise Architecture standard.

Standards bodies continue to promote the expansion of LDAP towards the complexity of DAP as new critical directory access requirements are identified in the marketplace. LDAP Version 3 revisions (presently in draft standard form) along with LDAP schema proposals (also in draft standard form), define important aspects of directory design as part of defining how directory information is to be accessed.

If all enterprise directories were LDAP compliant, this would provide a foundation for the consolidation of directories across enterprise platforms regardless of the vendor mix. LDAP allows applications on different platforms to access one central directory using an open method instead of requiring that each platform provide its own redundant directory.

Improving and simplifying access to resources on a network can result in considerable timesaving and other efficiencies. Also, standardizing access methods can result in reduced learning curves for resource administrators (e.g., network administrators) and users (e.g., programmers and others). Use of centralized and distributed LDAP-compliant directories to provide access to network resources such as servers can be an enabler of applications such as "single sign-on passwords." Single sign-on is an example of an application that can both reduce costs and have potential for improving security (e.g., from users not writing down their multiple passwords and from more efficient privilege removal).

The Internet provides numerous resources for agencies that are interested in learning more about LDAP directories. Agencies may wish to consider the following aspects of directory design, deployment and access.

1. Agencies are encouraged to consider their enterprise-wide needs for directory services. When the service need spans multiple agencies, directory services should be developed jointly by the involved agencies.
2. Agencies are encouraged to consider the potential interplay among directories, registries, and relational databases within their computing environment. The following sets of slides from presentations by Steve Kille and Jeff Hodges provide a good discussion of these relationships. These individuals were instrumental in the rollout of directories and registries at Stanford University.

Steve Kille:

http://www.stanford.edu/~hodges/talks/EMA98-DirectoryServicesRollout/Steve_Kille/sld001.htm).

Jeff Hodges:

<http://www.stanford.edu/~hodges/talks/OpenGroupApril98/StanfordRegistryAndDirectory/sld002.htm>).

3. Agencies are encouraged to review example directory development efforts as these may provide instructive roadmaps and lessons learned. Central directory development efforts at Stanford University and by Educause are described in considerable detail and may be accessed at the sights provided below.

The Directory Services Project at Stanford University:

<http://www.stanford.edu/group/networking/directory/directory.html>).

The Registry Project at Stanford:

<http://www.stanford.edu/group/itss-ccs/project/registry/>).

Educause person schema development:

<http://www.educause.edu/eduperson>).

4. Agencies are encouraged to review the IBM Redbook "how to" guide to LDAP Directories. This manual has implications for efforts that are not IBM

efforts. The manual is available at <http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg244986.html?Open>.

5. Agencies are encouraged to address security threats to LDAP directory accessibility and to the information stored in LDAP directories. The Systems Administration and Network Security Institute (SANS) provides a good article explaining LDAP and security issues related to it.

Overview & Security Aspects of the Lightweight Directory Access Protocol (LDAP), Louis R. Brand, April 17, 2001:
<http://www.sans.org/infosecFAQ/authentic/LDAP.htm>.

6. LDAP directory services are increasingly available on all major platforms (e.g., Netscape, Sun, Microsoft, Novell, IBM, etc.), but some implementations are more usable than others. Agencies are encouraged to check the literature for recent comparative articles. One example article is provided below, not as a definitive critique, but as an example commentary. This article provides an excellent list of reasons for centralizing the network's "who, what, and where" information. It suggests that the platform for that centralization effort should be the one that provides ease of administration.

Windows 2000 directory gains ground on NetWare, Unix - A Computer World magazine article.

http://www.computerworld.com/cwi/story/0,1199,NAV47_STO33219,00.html.

Requirement 2. Messaging Protocol Standards

State agency email messaging must be SMTP/ESMTP and MIME compatible. Local governments also are encouraged to follow these standards requirements.

Email systems presently in use in state and local government and in universities may already meet the requirements of being SMTP/ESMTP and MIME compatible. Compatibility with these protocols means that electronic mail conforms to Internet Engineering Task Force (IETF) standards in its envelope and content structures thus making email messages easily transported from one SMTP email host to another (i.e., server-to-server communications) and readable by any compliant email clients with appropriate extensions.

ESMTP or Extended Simple Mail Transfer Protocol is a method for introducing new functionality to SMTP email. ESMTP may enable easier retrieval of email from an ISP or use of a more complex set of potential attachments. For example, if the voicemail server were to send "mail" to the email server so that all of the mail from a particular group of customers could be intermingled and ordered by time of receipt, the voicemail and email would need compatible headers and bodies. This would enable recognition of both types of mail by the user's "combination mail" client. The integration of voice and electronic mail is an actual ESMTP example that is called VPIM or voice profile for Internet mail. VPIM is explained in ten IETF Internet drafts addressing voicemail. These drafts may be viewed at: <http://www.ietf.org/ids.by.wg/vpim.html>. The future

integration of voice and data on computer networks is an excellent example of why it is important to standardize on SMTP.

MIME means multipurpose Internet mail extension. MIME file type extensions may be used to indicate the content type of email attachments in email envelopes or to specify type within content headers of Web pages (e.g., content length, type, location and encoding). A document content type might be image or audio, for example, and encoding might be binary or US ASCII. Type indicators such as “*.gif” also aid in establishing a connection between the sent document and the local application that may be used to open the document type. Extensions are registered with IANA, the Internet Assigned Numbers Authority, a registry of codes and numbers used in discussing the Internet.

Resources

Standard Groups

The resources identified below are primarily standards groups involved in LDAP, SMTP, or middleware.

EDUCAUSE/Internet2 eduPerson task force has the mission of defining an LDAP object class (LDAP Schema) that includes widely used person attributes in higher education (<http://www.educause.edu/eduperson>).

IANA is the Internet Assigned Numbers Authority controls numbers and names including those related to mail extensions (e.g., image and .gif) and RFCs (e.g., RFC 2045 addresses MIME). This is a good place to glance at topics being addressed (<http://www.iana.org/>).

The IETF is the standards group that addresses LDAP directory standards (<http://www.ietf.org/>).

Internet 2 addresses middleware including directories, authentication, and security (<http://www.internet2.org/>).

The Internet Mail Consortium addresses messaging. The IMC also provides an excellent explanation of Internet Drafts versus Internet standards (<http://www.imc.org/mail-standards.html>).

The International Telecommunications Union or ITU-T maintains the X.500 series of publications and developer's guides (<http://www.itu.org/> or <http://www.itu.int/rec/recommendation.asp?type=products&lang=e&parent=T-REC-X>).

LDAP

The resources below include detailed information on LDAP requests for comment (RFCs) and LDAP related white papers.

LDAP standards are sets of RFCs overseen by IETF chartered groups. The IETF has several active LDAP working groups with multiple drafts traversing the standards adoption process.

LDAP Version 3: [LDAP \(v3\) Revision \(ldapbis\)](#)—9 Internet Drafts

LDAP Extensions: [LDAP Extension \(ldapext\)](#)—12 Internet-Drafts

Replication of Distributed LDAP Directories: [LDAP Duplication/Replication/Update Protocols \(ldup\)](#)—8 Internet-Drafts

The IETF also maintains information on inactive working groups.

IETF lsd—LDAP Service Deployment Charter (inactive working group).
<http://www.ietf.org/html.charters/OLD/lsd-charter.html>

The Open Group is concerned with X.400 messaging and the X.500 directory and LDAP access to it. This group provides relevant white papers and maintains several related forums as noted below:

White paper (<http://www.opengroup.org/directory/branding/0006/wp04.pdf>)

Directory Interoperability Forum (<http://www.opengroup.org/directory/>)

Electronic Messaging Forum (<http://www.ema.org/>)

Mobile and Directory Working Group
(<http://www.opengroup.org/mobile/mmfdfwg.htm>)

The LDAP Zone offers product development information (<http://www.ldapzone.com/>).

Internet 2 addresses directories and other middleware issues at
<http://middleware.internet2.edu/>.

MIME

The IETF describes current MIME RFCs as follows:

The initial document, RFC 2045, specifies the various headers used to describe the structure of MIME messages.

<http://www.ietf.org/rfc/rfc2045.txt?number=2045>

The second document, RFC 2046, defines the general structure of the MIME media typing system and defines an initial set of media types.

<http://www.ietf.org/rfc/rfc2046.txt?number=2046>

The third document, RFC 2047, describes extensions to RFC 822 to allow non-US-ASCII text data in Internet mail header fields.

<http://www.ietf.org/rfc/rfc2047.txt?number=2047>

The fourth document, RFC 2048, specifies various IANA registration procedures for MIME-related facilities. <http://www.ietf.org/rfc/rfc2048.txt?number=2048>

The fifth and final document, RFC 2049, describes MIME conformance criteria as well as providing some illustrative examples of MIME message formats, acknowledgements, and the bibliography.

<http://www.ietf.org/rfc/rfc2049.txt?number=2049>

SMTP/ESMTP

The Internet Mail Consortium (IMC) provides information on mail standards including SMTP and MIME.

SMTP Standards are listed under Host-To-Host Mail Transfer at:

<http://www.imc.org/rfcs.html#hosttohost>

MIME Standards are provided under Multipurpose Internet Mail Extensions (MIME) at: <http://www.imc.org/rfcs.html#mime>

SMTP Drafts are listed under Host-To-Host Mail Transfer at:

<http://www.imc.org/ids.html#hosttohost>

MIME Drafts are provided under Multipurpose Internet Mail Extensions (MIME) at: <http://www.imc.org/ids.html#mime>

Requesting Waivers to Requirements

Under certain circumstances, waivers from the provisions of this standard may be granted to state agencies if compliance with the provisions of this standard would:

- adversely affect the accomplishment of the agency mission; or
- cause a major adverse financial impact which is not offset by Government wide savings.

Written waiver requests shall be submitted to:

Director
Department of Technology Planning
Richmond Plaza, 110 S. 7th Street
Richmond, VA 23219

The Department of Information Technology shall provide information and technical expertise to assist the Director in making decisions on wavier requests.

Glossary

Directory — A simple list or a more complex database, usually created for finding resources in a networked environment.

Directory Services — The purposes for which network directories are created. Directories typically contribute information that is instrumental in providing and restricting access to resources on a network. Examples of directory services are file access, server access, single system-wide logon for access to all network resources, user access to resources, and access to person information.

Lightweight Directory Access Protocol (LDAP) — LDAP specifies how directories are accessed. LDAP is a simplified, TCP/IP-model-oriented version of DAP. DAP is the X.500 directory access protocol.

MIME - Multipurpose Internet Mail Extension

N-tier – N-tier describes the result of designing applications purposefully to function across various clients, servers and databases in a networked environment instead of on just one server or on a mainframe. For example, a “two-tiered environment” is an environment where client applications interact with a database server directly. A three-tiered environment might mean a remote Internet user’s browser application on the user’s machine is interacting with a Web application server, which in turn, is interacting with a database server. N-tiers can reference more complex arrangements and related groups of servers.

Simple Mail Transfer Protocol/Extended Simple Mail Transfer Protocol (SMTP/ESMTP) — SMTP is a protocol documented in RFC 2821 that relays an object including an envelope and content (i.e., relays

from host to host). The envelope includes an originator address, a mode of delivery and one or more delivery addresses. Content has a US ASCII header (structured according to RFC822) and a body that may be structured as US ASCII or MIME. RFC1869 provides for the extension of SMTP by designating how a client and a server may communicate the mutual recognition of an extension.

Voice Profile for (Internet) Mail (VPM) - The VPIM version 2 profile was developed by a non-IETF group, the electronic messaging association (EMA) and is now a workgroup of the IETF (see also <http://www.ema.org/vpim/>). VPIM v2 provides an extension to SMTP that will bridge present voice systems and email systems to enable voice and fax integration with email. The IETF references VPIM v2 as RFC 2421. Version 2 focused on changes required to voice platforms to route voice on the Internet in the manner that is compliant with SMTP. This version is being implemented by voicemail providers. Version 3 is under development to minimize the changes required to present day email systems to receive and send voice messages. VPIM v3 treats voice as a module of email. VPIM is an extension of SMTP (ESMTP).

X.400 - The set of International Telecommunications Union (ITU and also ITU-T) standards for electronic mail services provided by data networks. ITU-T was formerly Comité Consultatif International de Télégraphique et Téléphoniques or CCITT.

X.500 — The set of ITU-T standards for creating directories and providing access to them.

Appendix A: Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines

The Department of Technology Planning is responsible for assigning a uniform alphanumeric Publication Designation (PD) to all Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Policies, Standards, and Guidelines (PSG). The PD is derived, in part, from components of the Commonwealth Enterprise Architecture (EA) known as “Infrastructure Domains.” The “Infrastructure Domains” and Governance are defined in the [Commonwealth EA Glossary](#). The Governance code is used to identify those PSG that are not uniquely related to a specific infrastructure domain, e.g. “IT Project Management” or “IT Project Oversight.”

The following alpha codes will be used to identify each PSG:

Infrastructure Domains + Governance

Code

Governance and Transitional Processes	GOV
Platform Architecture	PLA
Database Architecture	DAT
Network Architecture	NET
Security Architecture	SEC
Systems Management Architecture	SYS
Information Architecture	INF
Application Architecture	APP
Middleware Architecture	MID

Publication Designations are constructed as follows:

COV ITRM (“Policy,” “Standard,” or “Guideline”) XXXYYYY-ZZZ

Where: XXX is the assigned Infrastructure Domain + Governance code;
YYYY is the year of initial issue; and
ZZZ is the sequential number assigned to link related PSG.

Example: COV ITRM Standard GOV2000-01.1 is a standard that implements
COV ITRM Policy GOV2000-01.1.