Ontario

Government of Ontario

Government of Ontario IT Standard (GO-ITS)
Number 24.2
Omnibus Technical Standard

Version #: 3.0
Status: APPROVED

Prepared for the Information Technology Standards Council (ITSC) under the delegated authority of the Management Board of Cabinet

Last Review Date: 2008-01-16
Next Review Date: 2008-07

Foreword

Government of Ontario Information Technology Standards (GO-ITS) are the official publications on the guidelines, preferred practices, standards and technical reports adopted by the Information Technology Standards Council (ITSC) under delegated authority of the Management Board of Cabinet (MBC). These publications support the responsibilities of the Ministry of Government and Consumer Services (MGCS) for coordinating standardization of Information & Information Technology (I&IT) in the Government of Ontario. Publications that set new or revised standards provide enterprise architecture guidance, policy guidance and administrative information for their implementation. In particular, GO-ITS describe where the application of a standard is mandatory and specify any qualifications governing the implementation of standards.

Last Review Date: 2008-01-16
Next Review Date: 2008-07

Table of Contents

1. Introduction

1.1 Background and Purpose

The Omnibus standards; 24.0, 24.1 and 24.2 provide the foundation for the realization of an open and interoperable I&IT environment in the OPS. Each of the Omnibus standards promotes the use of open standards developed by recognized standards development organizations and consortiums. They each provide an integrated set of standards designed to work together to support solution interoperability within the two standardized OPS environments (.NET and Java).

Omnibus 24.2 defines the key technical standards for networking and connectivity. Omnibus 24.0 defines a web services interface environment and 24.1 defines the information, content and presentation environment. Together these standards position the OPS to take advantage of Service Oriented Architecture (SOA) frameworks in the future, which hold the greatest potential for lowering integration costs and increasing flexibility across multiple solutions in a shared (consolidated) infrastructure environment.

The Omnibus standards align with, and are designed to be implemented with, other important Government of Ontario IT Standards including **GO-ITS 54 *Application Development Standard*** which specifies application development requirements in the OPS, **GO-ITS 20.1 *Platform Software Standard*** which defines the two OPS standardized IT environments (.NET and Java), and **GO-ITS 23.1 *Government of Ontario Public Web Standard*.**

1.2 Target Audience

GO-ITS 24 Omnibus Interoperability Standard applies to all Government of Ontario technology solutions providers, application development and integration.

1.3 Scope

This standard focuses on key interoperability standards that impact the communications infrastructure. Other standards that impact interoperability will be addressed by other GO-ITS documents, or are represented by standards documentation provided by communications infrastructure solution providers such as ITS.

1.3.1 In Scope

- Technical standards from recognized national and international Standards Development Organizations (SDOs)

1.3.2 Out of Scope

- Architecture best practices, frameworks, governance, methodologies and principles related to Service-Oriented Architecture (SOA)

- Information use, retention, disclosure and disposal policies, regulations or statutes that apply to the OPS, as well as any information asset safeguarding requirements of the OPS (e.g., Statutes, legislation, regulations or OPS-specific directives or standards regarding I&IT security and privacy)
- Monitoring and compliance mechanisms for adherence to this standards document
- Service Level Agreements (SLAs), performance metrics and quality assurance measures

1.4 Applicability Statements

1.4.1 Organization

Government of Ontario IT Standards and Enterprise Solutions and Services apply (are mandatory) for use by all ministries/clusters and to all former Schedule I and IV provincial government agencies under their present classification (Advisory, Regulatory, Adjudicative, Operational Service, Operational Enterprise, Trust or Crown Foundation) according to the current agency classification system.

Additionally, this applies to any other new or existing agencies designated by Management Board of Cabinet as being subject to such publications, i.e. the GO-ITS publications and enterprise products - and particularly applies to Advisory, Regulatory, and Adjudicative Agencies (see also procurement link, OPS paragraph). Further included is any agency which, under the terms of its Memorandum of Understanding with its responsible Minister, is required to satisfy the mandatory requirements set out in any of the Management Board of Cabinet Directives (*cf*. Operational Service, Operational Enterprise, Trust, or Crown Foundation Agencies).

As new GO-IT standards are approved, they are deemed mandatory on a go-forward basis (Go-forward basis means at the next available project development or procurement opportunity).

When implementing or adopting any Government of Ontario IT standards or IT standards updates, ministries and I&IT Cluster must follow their organization's pre-approved policies and practices for ensuring that adequate change control, change management and risk mitigation mechanisms are in place and employed.

For the purposes of this document, any reference to ministries or the Government includes applicable agencies.

Refer to section 2.0 *Compliance Requirements* for more information.

1.5 Requirements Levels

Within this document, certain wording conventions are followed. There are precise requirements and obligations associated with the following terms:

Must	This word, or the terms "REQUIRED" or "SHALL", means that the statement is an absolute requirement.
Should	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore the recommendation, but the full implications (e.g., business functionality, security, cost) must be understood and carefully weighed before

1.6 Recommended Versioning and/or Change Management

Each of the three Omnibus Standards package together many inter-related standards that have developed by several different standards development organizations and consortiums. The individual standards development organizations will each be monitored for changes (minor and substantive) to their respective standards and specifications on a regular basis, every 6 months. As they evolve, the Omnibus standard that references them will also be updated to reflect the changes. When the changes collectively, reach a stage where they have a material impact on the implementation of the standard, then the respective Omnibus standard will be brought forward to Information Technology Standards Council (ITSC) and the Architecture Review Board (ARB) for review and approval, as per the approved governance process for all Government of Ontario IT Standards (GO-ITS).

It is important to note that, as with all GO-ITS, the Omnibus standards are meant to align with, and support other, related GO-ITS such as the **GO-ITS 20.1 *Platform Software Standard***, therefore if there are updates made to related standards this may also trigger updates to the Omnibus standards.

1.7 Publication Details

All approved Government of Ontario IT Standards (GO-ITS) are published on the ITSC Intranet web site. Please indicate with a checkmark below if this standard is also to be published on the public, GO-ITS Internet Site.

Standard to be published on both the OPS Intranet and the GO-ITS Internet web site (available to the public, vendors etc.)	☑

2. Compliance Requirements

All OPS projects/solutions proceeding through the Corporate Gating Process must demonstrate their alignment with the key technology standards outlined in this document.

Section 3.0 of this document lists key standards that are relevant to communications. The standards listed here are considered “key” for one of two reasons:

- They are critical for supporting the implementation of web services (as specified in GO-ITS 24.1), or
- There are multiple options and the OPS are recommending the adoption of a specific standard for specific reasons.

It is not necessary to detail all of the I&IT communications standards because the list would be unwieldy and in many cases these standards are not relevant to project teams; the communications services are usually provided by the OPS infrastructure service provider, ITS, and those services would necessarily be compliant with the standards deemed necessary by ITS.

Take as an example a project that requires wireless communications in order to support their solution. The default option in this case would be to select 802.11g-compliant hardware because the “g” specification is the most current approved standard. The reason that 802.11g has been identified as a “key” standard in this document is because although the “g” specification has been selected as the standard, we need to emphasize that the “n” specification is going to be ratified imminently and so project teams are recommended to purchase hardware that supports both the “g” and the future “n” specifications of 802.11.

3. Mandatory Requirements

3.1 Key Transport Standards

3.1.1 HyperText Transfer Protocol (HTTP) Version 1.1

Title HyperText Transfer Protocol (HTTP)
Version 1.1
Sponsor W3C/IETF

Description
The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes and headers [47]. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred.

Industry Standards http://www.w3.org/Protocols/rfc2616/rfc2616.html
Publication Date 1999-06

3.1.2 Secure Socket Layer (SSL) Version 3.0

Title Secure Socket Layer (SSL)
Version 3.0
Sponsor Netscape

Description
This document specifies Version 3.0 of the Secure Sockets Layer (SSL V3.0) protocol, a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP[TCP]), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently.

Industry Standards http://wp.netscape.com/eng/ssl3/draft302.txt
Publication Date 1996-11-18

3.1.3 Transport Layer Security (TLS) Version 1.0

Title Transport Layer Security (TLS)
Version 1.0
Sponsor IETF

Description
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers.

The TLS protocol allows applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications privacy over the Internet using cryptography. Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (whether an individual or an application, such as a Web browser) can be sure with whom they are communicating.

The next level of security—in which both ends of the "conversation" are sure with whom they are communicating—is known as mutual authentication. Mutual authentication requires public key infrastructure (PKI) deployment to clients unless TLS-PSK or TLS-SRP are used, which provide strong mutual authentication without needing to deploy a PKI.

Industry Standards http://tools.ietf.org/html/rfc2246
Publication Date 1999-06

3.1.4 Simple Mail Transfer Protocol (SMTP)

Title Simple Mail Transfer Protocol (SMTP)
Version RFC2821
Sponsor IETF

Description
Simple Mail Transfer Protocol (SMTP) is the de facto standard for e-mail transmissions across the Internet.

SMTP is a relatively simple, text-based protocol, in which one or more recipients of a message are specified (and in most cases verified to exist) along with the message text and possibly other encoded objects. The message is then transferred to a remote server using a procedure of queries and responses between the client and server.

Industry Standards http://tools.ietf.org/html/rfc2821
Publication Date 2001-April

3.1.5 File Transfer Protocol (FTP)

Title File Transfer Protocol
Version RFC959
Sponsor IETF

Description
FTP or File Transfer Protocol is used to transfer data from one computer to another over the Internet, or through a network.

Specifically, FTP is a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol (such as the Internet or an intranet). This allows any computer connected to a TCP/IP based network to manipulate files on another computer on that network regardless of which operating systems are involved.

Industry Standards http://www.apps.ietf.org/rfc/rfc959.html
Publication Date 1985-10

3.1.6 Java Message Service (JMS) Version 1.1

Title Java Message Service (JMS)
Version 1.1
Sponsor Java Community Process

Description
The Java Message Service (JMS) API is a Java Message Oriented Middleware (MOM) API for sending messages between two or more clients. The JMS API defines a common set of messaging concepts and programming strategies that will be supported by all JMS technology-compliant messaging systems.

Industry Standards http://www.jcp.org/en/jsr/detail?id=914
Publication Date 2003-12-02

3.1.7 Internet Inter-Orb Protocol (IIOP) Version 3.03

Title Internet Inter-Orb Protocol (IIOP)
Version 3.03
Sponsor The Object Management Group

Description
IIOP (Internet Inter-ORB Protocol) is a protocol that makes it possible for distributed programs written in different programming languages to communicate over the Internet. IIOP is a critical part of the Common Object Request Broker Architecture (CORBA). Using CORBA's IIOP and related protocols, a company can write programs that will be able to communicate with their own or other company's existing or future programs wherever they are located and without having to understand anything about the program other than its service and a name.

Industry Standards http://www.omg.org/technology/documents/formal/corba_iiop.htm
Publication Date 2004-03-01

3.1.8 Blocks Extensible Exchange Protocol (BEEP)

Title Blocks Extensible Exchange Protocol
Version RFC3080
Sponsor IETF

Description
BEEP (Blocks Extensible Exchange Protocol) is a framework for creating network application protocols. It is intended to abstract out the common features that have traditionally been duplicated in each protocol implementation. BEEP (formerly called BXXP) typically runs on top of TCP and allows the exchange of messages called 'frames'. Unlike HTTP (and similar protocols), either end of the connection can send a frame at any time, and 'questions' and 'replies' can be interleaved easily. BEEP also includes facilities for encryption and authentication and is highly extensible. Key functionality afforded by BEEP is the enablement of simultaneous and independent exchanges within the context of a single application user-identity, supporting both textual and binary messages.

Industry Standards http://tools.ietf.org/html/rfc3080
Publication Date 2001-03

3.1.9 RTP: A Transport Protocol for Real-Time Applications

Title RFC3550: RTP: A Transport Protocol for Real-Time Applications
Sponsor IETF

Description
RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers.

Industry Standards http://www.apps.ietf.org/rfc/rfc3550.html
Publication Date 2003-07

3.1.10 Domain Name System (DNS)

Title Domain Name System (DNS)
Version RFC1034, RFC1035
Sponsor IETF

Description
The Domain Name System protocol specifies a consistent namespace for referring to resources on the internet.

The specification defines three major components:

- The Domain Name Space, which specifies a tree-based directory.
- Name Servers, which are server programs that contain the information about the domain tree's structure and information set.
- Resolvers, which are programs that extract information from name servers in response to user requests.

Industry Standards http://tools.ietf.org/html/rfc1034
http://tools.ietf.org/html/rfc1035
Publication Date 1987-11

3.1.11 Wireless Application Protocol (WAP)

Title Wireless Application Protocol (WAP)
Sponsor Open Mobile Alliance

Description
WAP is an open international standard for applications that use wireless communication. Its principal application is to enable access to the Internet from a mobile phone or PDA.

A WAP browser provides all of the basic services of a computer based web browser but simplified to operate within the restrictions of a mobile phone. WAP sites are websites written in, or dynamically converted to, WML (Wireless Markup Language) and accessed via the WAP browser.

Associated Specifications

- Wireless Application Protocol-User Agent Profiling
- Wireless Application Protocol-Service Loading
- Wireless Application Protocol-Service Loading SIN
- Wireless Application Protocol-Service Indication
- Wireless Application Protocol-Service Indication SIN
- Wireless Application Protocol-Push OTA
- Wireless Application Protocol-Push OTA SIN
- Wireless Session Protocol
- Wireless Transaction Protocol
- Wireless Datagram Protocol
- Wireless Control Message Protocol
- Wireless Markup Language (WML)
- Wireless Script Language and Wireless Script Language SIN

Industry Standards http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html
Publication Date 2001-07-12

3.1.12 Session Initiation Protocol (SIP)

Title Session Initiation Protocol
Sponsor IETF

Description
Session Initiation Protocol (SIP) is an application-layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants.

These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols.

Industry Standards http://tools.ietf.org/html/rfc3261
Publication Date 2002-06

3.2 Key Internet Standards

3.2.1 Internet Protocol Version 4 (IPv4)

Title Internet Protocol (IP)
Version 4, RFC791
Sponsor IETF

Description
The Internet Protocol specification is the key communications protocol for the OPS, and for the internet. IPv4 is a data-oriented protocol to be used on a packet switched internetwork (e.g., Ethernet). The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks.

The pool of available Internet Protocol addresses is gradually being exhausted, and is expected to run out sometime in the next 5-10 years.

Note that the successor to IPv4 is already being deployed and will provide a significant change to the base internet protocol suite. IPv6 provides an expanded address space which will address the problem of the dwindling availability of IPv4 addresses.

Industry Standards http://tools.ietf.org/html/rfc791
Publication Date 1981-09

3.2.2 Transmission Control Protocol (TCP)

Title Transmission Control Protocol (TCP)
Version RFC793
Sponsor IETF

Description
The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite. TCP provides reliable, in-order delivery of a stream of bytes, making it suitable for applications like file transfer and e-mail. It is so important in the Internet protocol suite that sometimes the entire suite is referred to as "the TCP/IP protocol suite."

Industry Standards http://tools.ietf.org/html/rfc793
Publication Date 1981-09

3.2.3 User Datagram Protocol (UDP)

Title User Datagram Protocol (UDP)
Version RFC793
Sponsor IETF

Description
The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as datagrams (using Datagram Sockets) to one another. UDP does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order, appear duplicated, or go missing without notice. Avoiding the overhead of checking whether every packet actually arrived makes UDP faster and more efficient for applications that do not need guaranteed delivery.

Common network applications that use UDP include the Domain Name System (DNS), and streaming media applications such as IPTV, Voice over IP (VoIP).

Industry Standards http://tools.ietf.org/html/rfc793
Publication Date 1981-09

3.3 Key Network Access Standards

3.3.1 802.11-2007 Wireless LAN Specifications

Title Wireless LAN Specifications
Sponsor IEEE

Description
IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz spectrum.

Industry Standards http://www.ieee802.org/11/
Publication Date 2007-03-08

3.3.2 802.11g Wireless LAN Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band

Title 802.11g Wireless LAN Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band
Sponsor IEEE

Description
802.11g is the third modulation standard of the original 802.11 specification. This works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 19 Mbit/s net throughputs. 802.11g hardware is fully backwards compatible with 802.11b hardware.

Note that the “n” specification of the 802.11 standard is in the process of being ratified, and project teams are encouraged to procure hardware that supports both the “g” and the imminent ratified “n” specifications of the standard. Please refer to the Technology Standards Roadmap, Section xx for more information.

Industry Standards http://www.ieee802.org/11/
Publication Date 2003-06

3.3.3 Category 6 Cabling (TIA/EIA-854)

Title Category 6 Cabling (TIA/EIA-854)
Sponsor TIA/EIA

Description
Category 6 cable, commonly referred to as Cat 6, is a cable standard for Gigabit Ethernet and other network protocols that is backward compatible with the Category 5/5e and Category 3 cable standards. Cat-6 features more stringent specifications for crosstalk and system noise. The cable standard provides performance of up to 250 MHz and is suitable for 10BASE-T / 100BASE-TX and 1000BASE-T (Gigabit Ethernet). It is expected to suit the 10GBASE-T (10Gigabit Ethernet) standard, although with limitations on length if unshielded Cat 6 cable is used.

Industry Standards
http://www.tiaonline.org/standards/catalog/search.cfm?standards_criteria=Category%206
Publication Date 2001-06

4. Related Standards

4.1 Impacts to Existing Standards

GO-ITS	Describe Impact	Recommended Action (alternatively provide a page number where details can be found)
GO-ITS 39.1 Wireless Local Area Networks (LANs) Version 1.0	The IEEE standard 802.11-2007 referenced here will update the 802.11i specification listed for wireless LANs in GO-ITS 39.1	GO-ITS 39.1 Version 1.0 will need to be retired as new security GO-ITS come forward addressing encryption methods used in the OPS
GO-ITS 80.00 Wiring Topology for Government Buildings	Category 6 cable is the new mandated level for network wiring in the OPS	See page 15

4.2 Impacts to Existing Environment

Impacted Infrastructure (includes Common Components and other applications)	Describe Impact	Recommended Action (alternatively provide a page number where details can be found)
Network Wiring	New or refurbished network wiring initiatives must deploy Category 6 cabling on a go-forward basis	See page 15
Network Applications and Hardware	Network-based applications that currently conform to GO-ITS 24 will not be affected since GO-ITS standards apply only to new product and solution deployments.	All documents referencing GO-ITS 24 Version 2.0 should be updated to reference this revised version, namely, GO-ITS 24.2 Omnibus Technical Standard Version 3

5. Contact Information

	Contact 1	Contact 2
Full Name:	Doretta Ojeda	TBA
Job Title:	Standards Program Coordinator	Technical Coordinator
Organization:	Ministry of Government Services and Consumer Services (MGCS)	Ministry of Government Services and Consumer Services (MGCS)
Division:	Office of the Corporate Chief Technology Officer (OCCTO)	Office of the Corporate Chief Technology Officer (OCCTO)
Branch:	Technology Adoption Branch	Technology Adoption Branch
Office Phone:	416-327-2094	416-212-0940
E-mail Address:	doretta.ojeda@ontario.ca	

6. Acknowledgements

6.1 Editors

Full Name	Cluster, Ministry and/or Area
Technical Coordinator	OCCTO

6.2 Contributors

Full Name	Cluster, Ministry and/or Area
Richard Budel	IBM Canada
Brian Bisaillon	OCCTO
Paul Daly	OCCTO

7. Document History

Created: 2007-11-23

Approved: 2008-01-16

- Approved by the IT Standards Council as an update to previous Omnibus Technical Standard dated January 2005

8. Copyright Information