Standards, Policies and Guidelines - Malaysian Government Interoperability Framework (MyGIF)

MAMPU

Version 1.0

August 2003

TABLE OF CONTENTS

1. INTRODUCTION

This report documents the detail recommendations resulting from the research and analysis conducted in the development of the Malaysian Government Interoperability Framework (MyGIF). It contains information of ICT standards and technical specifications recommended for adoption in the MyGIF.

1.1 Definition

MyGIF defines the minimum set of collection of ICT standards and technical specifications governing the communication of systems, flow of information, as well as the exchange of data and business processes that relates to Government Ministries, agencies and departments.

MyGIF basically covers the following five (5) interoperability areas:

- Interconnection;
- Data Integration;
- Information Access;
- Security; and
- Metadata.

Instead of creating new standards or specifications, MyGIF adopts internationally recognised open and *de facto* ICT standards as well as technical specifications for all the interoperability areas mentioned.

1.2 Objectives

MyGIF's objectives are:

- To enable different Government systems and applications, both within Government and external to Government, communicate and interoperate efficiently and effectively;
- To promote and foster the adoption of Extensible Markup Language (XML) that enables the exchange of data between applications;
- To promote the addition and use of Metadata, i.e. Data Dictionary Sektor Awam (DDSA), to Government information resources;
- To align with the Internet by adoption of common specifications used on the Internet and World Wide Web for all Government information systems; and
- To adopt Open standards and specifications that are widely supported by the market in order to reduce the total cost of ownership of Government information systems.

1.3 Key Drivers

The key drivers guiding the recommendations of ICT standards and technical specifications for MyGIF are:

- Interoperability
  - Standards and specifications recommended must be relevant to the five interoperability areas specified above, i.e. Interconnection, Data Integration, Information Access, Security, and Metadata.
- Maturity and Popularity
  - Standards and specifications recommended should be internationally recognized or *de facto* standards that are matured and widely used in the IT industry.

- Market Support
  - Standards and specifications recommended should be widely supported by the dominant technology platforms, software packages and business applications in the market.
- Open Standard
  - Standards and specifications recommended should be open standards as far as possible. Standards that are vendor and product neutral should be considered in favour of their proprietary alternatives.
- Internet
  - Standards and specifications recommended should be well aligned with the Internet standards (e.g. W3C and IETF) since the Internet is a major delivery channel for the Government information resources and services.
- Existing Government Policies and Standards
  - Standards and specifications recommended must be complied with the existing Government policies and standards wherever relevant.
  - Existing published Government policies and standards that are relevant to be observed and complied are:

    1.3.1 Electronic Government Information Technology Policy & Standards (EGIT) version 1.0, published on 1 July 1997.

    1.3.2 The Malaysian Public Sector ICT Management Security Handbook (MyMIS) published in January 2002.

    1.3.3 Digital Signature Act 1997 and Digital Signature Regulations 1998.

1.4 Scope

MyGIF covers the communication of systems as well as the exchange of information between Government systems and the interactions between the following:

- Government-to-Government (G2G)
  - Within Malaysian Government and Public Sector, i.e. between Government agencies and departments.
- Government-to-Citizens (G2C)
  - Between Malaysian Government and its citizens.
- Government-to-Businesses (G2B)
  - Between Malaysian Government and businesses in the private sector, i.e. suppliers and contractors to the Government.
- Government-to-Other Governments
  - In between Malaysian Government and other governments or association of governments such as ASEAN and United Nation.

“Malaysian Government” referred here includes the Government Ministries and their agencies and departments, local authorities, statutory bodies and the wider Public Sector at large, such as public higher learning institutes and national health services.

MyGIF standards and specifications should be mandatory on all new system implementations that fall within the scope defined in this section. For legacy systems that fall within the scope defined, agencies will need to assess if any integration are required between the legacy systems and other systems. If it is determined that integration would be required, interfaces will need to be defined to allow such integration to take place.

2. RECOMMENDATIONS FOR INTERCONNECTION

2.1 Overview

Interconnection covers interoperability components and technical specifications required to enable communication between different systems and the exchange of information over the networking environment – both local area network (LAN) and wide area network (WAN) within the Public Sector, as well as the Internet at large.

Interoperability components covered in the Interconnection area include:

- Hypertext Transfer;
- File Transfer;
- Email Transport;
- Mailbox Access;
- Directory Access;
- Domain Name Services;
- Newsgroup Services;
- Network Transport;
- LAN / WAN Internetworking;
- Wireless LAN;
- Mobile Device Internet Access;
- Intra-Government Remote Services Delivery Protocol;
- Intra-Government Remote Services Description Language; and
- Intra-Government Remote Services Request Registry.

2.2 Recommended Standards / Specifications

2.2.1 Hypertext Transfer

Hypertext transfer protocol is required to define how messages are to be formatted and transmitted. It also defines the commands to be used by the servers and clients. It enables browser-based access to the Government's hypertext content such as web pages.

Recommended standard / specification:

- HTTP v1.1 – Hypertext Transfer Protocol version 1.1.

HTTP v1.1	
Description	HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. It is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
Reference	HTTP v1.1 is a proposed IETF standard defined in: ▪ RFC 2616 "Hypertext Transfer Protocol – HTTP/1.1"; and ▪ RFC 2817 "Upgrading to TLS Within HTTP/1.1"; – updated for the upgrades to Transport Layer Security (TLS) within HTTP v1.1.
Rationale for Selection	▪ HTTP is a global, matured and widely adopted standard. ▪ HTTP has been in use by the World Wide Web global information initiative since 1990. ▪ Version 1.1 is currently the most widely used and latest version of this standard. ▪ Widely adopted and supported by all web servers and browsers.

HTTP v1.1	
Limitation	No known limitation on use of this standard.

2.2.2 File Transfer

File transfer protocols are required to enable the transfer of files over the network and the Internet. These protocols enable both users within the Government agencies and departments as well as third parties such as the citizens, businesses and suppliers to download content or file from the Government's central server.

Recommended standards / specifications:

- FTP – File Transfer Protocol; and
- HTTP v1.1 – Hypertext Transfer Protocol (refer to Section 2.2.1 for introduction on HTTP v1.1).

FTP	
Description	The File Transfer Protocol (FTP) is a standard internet protocol to enable the exchange of files between computers on the Internet. It enables users to move large files of any sort (i.e., video clips, large documents, audio or multi-media clips) between computers.
Reference	FTP is a proposed IETF standard defined in RFC 959 "File Transfer Protocol (FTP)".
Rationale for Selection	▪ FTP is a global, matured and widely adopted standard. ▪ Widely adopted and supported by relevant products.
Limitation	No known limitation on use of this standard.

2.2.3 Email Transport

Email transport protocols are required to enable the sending of email messages between servers and from email clients to mail servers. These protocols are also required to enable the exchange of messages in languages with different character sets as well as emails with attachments.

Recommended standards / specifications:

- SMTP / MIME – Simple Mail Transport Protocol / Multipurpose Internet Mail Extensions.

SMTP / MIME	
Description	Simple Mail Transport Protocol (SMTP) is the protocol used to deliver or relay e-mail messages. Multipurpose Internet Mail Extensions (MIME) is a specification for enhancing the capabilities of standard Internet electronic mail. It offers a simple standardized way to represent and encode a wide variety of media types for transmission via Internet mail.

SMTP / MIME	
Reference	SMTP is a proposed IETF standard defined in: ▪ RFC 2821 “Simple Mail Transport Protocol”; and ▪ RFC 2822 “Internet Message Format”. MIME is a proposed IETF standard defined in: ▪ RFC 2045 “MIME Part 1: Format of Internet Message Bodies”; ▪ RFC 2046 “MIME Part 2: Media Types”; ▪ RFC 2047 “MIME Part 3: Message Header Extensions for Non-ASCII Text”; ▪ RFC 2048 “MIME Part 4: Registration Procedures”; ▪ RFC 2049 “MIME Part 5: Conformance Criteria and Examples”; ▪ RFC 2231 “MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations”; ▪ RFC 2387 “The MIME Multipart/Related Content-type”; ▪ RFC 2392 “Content-ID and Message-ID Uniform Resource Locators”; ▪ RFC 2557 “MIME Encapsulation of Aggregate Documents”; and ▪ RFC 3023 “XML Media Type”.
Rationale for Selection	▪ SMTP/MIME are globally recognised, matured and widely adopted standards. ▪ Widely supported by common email packages such as Netscape Messenger, Microsoft Outlook and Outlook Express, and Lotus Notes.
Limitation	No known limitation on use of this standard.

2.2.4 Mailbox Access

Mailbox access protocols are required to enable remote access to email boxes at mail servers. These protocols enable users of Government agencies and departments access and download their emails at their office workplace or at home from the central mail servers.

Recommended standards / specifications:

- POP3 – Post Office Protocol version 3; and
- IMAP4rev1 – Internet Message Access Protocol version 4 rev1.

POP3	
Description	POP3 is a client/server protocol that intended to permit a workstation to dynamically access a mail held on a server host in a useful fashion. Usually, this means that the POP3 protocol is used to allow a workstation to retrieve emails that the server is holding for it.
Reference	POP3 is a proposed IETF standard defined in: ▪ RFC 1939 “Post Office Protocol - Version 3”; ▪ RFC 1957 “Some Observations on Implementations of POP3”; and ▪ RFC 2449 “POP3 Extension Mechanism”.
Rationale for Selection	▪ POP3 is the *de facto* protocol for retrieving mail from a mail server, due to its easy implementation, and simplicity of use. ▪ Widely supported by common email packages such as Netscape Messenger, Microsoft Outlook and Outlook Express, and Lotus Notes. ▪ POP3 will remain a dominant standard for remote mailbox access.

POP3	
Limitation	No known limitation on use of this standard.

IMAP4rev1	
Description	IMAP4 is a protocol that serves as a way to read mail on a remote host. Unlike POP3 which requires user to retrieve and download emails to a local email client (e.g. workstation), IMAP4 allows a client to access and manipulate email messages on the server. It permits manipulation of remote message folders, called “mailboxes”, in a way that is functionally equivalent to local mailboxes. It allows the same mail to be accessed from any location because all mail is stored on the server rather than on a user's computer. It also includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and clearing flags; searching; and selective fetching of message attributes, texts, and portions thereof. It also provides the capability for an offline client to resynchronize with the server.
Reference	IMAP4rev1 is a proposed IETF standard defined in: ▪ RFC 2060 “Internet Message Access Protocol - Version 4rev1”; ▪ RFC 2342 “IMAP4 Namespace”; and ▪ RFC 2971 “IMAP4 ID Extension”.

IMAP4rev1	
Rationale for Selection	▪ IMAP4 is a global, matured and widely adopted standard especially when required to support more advanced email functionality such as synchronization between client and server. ▪ Widely supported by major email clients and servers such as Microsoft Exchange, Netscape Messaging Server, Lotus Domino Mail Server. ▪ IMAP4 will remain a dominant standard for remote mailbox access.
Limitation	No known limitation on use of this standard.

2.2.5 Directory Access

Directory access protocol is required in order to define how to locate and access information stored in standard directories, i.e. directories that provide a centralised or distributed repository of organisation, organisational units (e.g. divisions and departments), people, IT resources (e.g. printers), together with associated attributes such as user name, printer name, email address, etc.

Recommended standard / specification:

- LDAP v3 – Lightweight Directory Access Protocol version 3.

LDAP v3	
Description	LDAP is designed to provide access to X.500 or other directories, with less resource usage required than Directory Access Protocol (DAP). It is specifically targeted at management applications and browser applications that provide read/write interactive access to directories.
Reference	LDAP v3 is a proposed IETF standard defined in: ▪ RFC 2251 “Lightweight Directory Access Protocol (v3)”; ▪ RFC 2252 “LDAPv3: Attribute Syntax Definitions”; ▪ RFC 2253 “LDAPv3: UTF-8 String Representation of Distinguished Names”; ▪ RFC 2254 “The String Representation of LDAP Search Filters”; ▪ RFC 2255 “The LDAP URL Format”; ▪ RFC 2256 “A Summary of the X.500(96) User Schema for use with LDAPv3”; ▪ RFC 2829 “Authentication Methods for LDAP”; ▪ RFC 2830 “LDAPv3: Extension for Transport Layer Security”; and ▪ RFC 3377 “LDAPv3: Technical Specification”.
Rationale for Selection	▪ LDAP is the dominant directory access protocol supported by all the major directory software providers. ▪ Version 3 is the latest version of LDAP and has been widely adopted.
Limitation	No known limitation on use of this standard.

2.2.6 Domain Name Services

Domain Name Service is required to enable location of an Internet address by name. In order to provide a meaningful and easy to use name for an Internet address, a domain name service provides a domain name server that maps those names to Internet addresses.

Recommended standard / specification:

- DNS – Domain Name System.

DNS	
Description	DNS is the way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address. DNS is a name resolution software that lets users locate computers (assigned with IP addresses) on the Internet by domain name. The DNS server maintains a database of domain names (host names) and their corresponding IP addresses.
Reference	DNS is a proposed IETF standard defined in: ▪ RFC 1034 "Domain Names - Concepts And Facilities"; ▪ RFC 1035 "Domain Names - Implementation And Specification"; and updated in: ▪ RFC 1101 "DNS Encoding of Network Names and Other Types"; ▪ RFC 1183 "New DNS RR Definitions"; ▪ RFC 1348 "DNS NSAP RRs"; ▪ RFC 1876 "A Means for Expressing Location Information in the Domain Name System"; ▪ RFC 1982 "Serial Number Arithmetic"; ▪ RFC 1995 "Incremental Zone Transfer in DNS"; ▪ RFC 1996 "A Mechanism for Prompt Notification of Zone Changes"; ▪ RFC 2136 "Dynamic Updates in the Domain Name System"; ▪ RFC 2137 "Secure DNS Dynamic Update"; ▪ RFC 2181 "Clarifications to the DNS Specification"; ▪ RFC 2308 "Negative Caching of DNS Queries";

DNS	
	▪ RFC 2535 “DNS Security Extensions”; and ▪ RFC 2845 “Secret Key Transaction Authentication for DNS”.
Rationale for Selection	▪ DNS is a global, matured and widely adopted standard. ▪ It is the dominant domain name service standard supported by all the relevant products.
Limitation	No known limitation on use of this standard.

2.2.7 Newsgroup Services

Newsgroup services are required to enable client access to newsgroups and manage notes posted to newsgroups. Newsgroups provide a forum for discussion about particular subjects. Notes are written and posted to a server and then distributed through a network of discussion groups. Newsgroups are organised into hierarchies, with major categories (e.g. Agency News), and sub-categories (e.g. MAMPU). The use of Newsgroup services may be subject to security constraints, for instance, allowing newsgroup traffic across government firewalls.

Recommended standard / specification:

- NNTP – Network News Transfer Protocol.

NNTP	
Description	NNTP specifies a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the Internet community. It is designed so that news articles are stored in a central database allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided.
Reference	NNTP is a proposed IETF standard defined in RFC 977 “Network News Transfer Protocol”.
Rationale for Selection	▪ NNTP is the predominant protocol used by computer clients and servers for managing the notes posted on Usenet newsgroups. It replaced the original Usenet protocol. ▪ It is a global, matured and widely adopted standard since it was introduced in 1986.
Limitation	No known limitation on use of this standard.

2.2.8 Network Transport

Network transport protocols works in conjunction with LAN/WAN internetworking protocols i.e. IP to allow data to be sent from one computer to another on a LAN, WAN or Internet. While IP handles the routing of packets (individual units of data) from one computer to another, network transport protocol such as TCP handles packet flow between systems.

Recommended standards / specifications:

- TCP – Transmission Control Protocol (preferred network transport protocol); and
- UDP – User Datagram Protocol (where required, subject to security constraints).

TCP	
Description	TCP is a protocol used along with the IP to send data in the form of message units between computers over the network. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the network. In contrast to UDP, TCP is a connection-oriented protocol, i.e. a virtual circuit is established between the two computers and ensures that packets are received in the same order in which they are transmitted. It also notifies the application if the connection between the two computers failed.
Reference	TCP is a proposed IETF standard defined in RFC 793 “Transmission Control Protocol”.
Rationale for Selection	▪ TCP is a global, matured and widely adopted standard that was introduced in 1991. ▪ Widely adopted by relevant products.
Limitation	No known limitation on use of this standard.

UDP	
Description	UDP is an alternative to TCP. It uses the IP to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, UDP is a connectionless protocol, therefore it does not divide a message into packets (datagrams) and reassemble it at the other end nor guarantee that messages will arrive at the destination in the correct sequence. These characteristics of UDP shows that it cannot be relied on for data delivery. UDP is preferred when network applications that want to save processing time (speed) because they have very small data units to exchange i.e. very little message reassembling to be done.
Reference	UDP is a proposed IETF standard defined in RFC 768 "User Datagram Protocol".
Rationale for Selection	▪ UDP is a matured standard that was filed in 1980. ▪ Widely adopted by relevant products.
Limitation	UDP is sometimes referred to as an unreliable protocol because when a program sends a UDP datagram over the network, there is no way for it to know that it actually arrived at it's destination. This means that the sender and receiver must typically implement their own application protocol on top of UDP. Much of the work that TCP does transparently (such as generating checksums, acknowledging the receipt of packets, retransmitting lost packets and so on) must be performed by the application itself.

2.2.9 LAN / WAN Internetworking

LAN/WAN Internetworking protocol is required to enable transmission of data from one computer to another on a LAN or WAN based on the computer's unique address on the network.

While network transport protocol such as TCP handles packet flow between systems, LAN/WAN Internetworking protocol handles the routing of packets (data) from one computer to another.

Recommended standard / specification:

- IPv4 – Internet Protocol version 4.

IPv4	
Description	IP is designed for use in interconnected systems of packet-switched computer communication networks. It provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses (IP addresses). In addition to inter network routing, IP provides error reporting and fragmentation and reassembly of information units called datagrams for transmission over networks with different maximum data unit sizes.
Reference	IP is a proposed IETF standard defined in RFC 791 "Internet Protocol".
Rationale for Selection	▪ IP is a global, matured and widely adopted standard since the transition to IPv4 took place in 1983. ▪ Version 4 is the current and most widely used version of IP.

IPv4	
Limitation	The number of addresses that can be supported by IPv4 is limited i.e. IP address size limited to 32 bits.

2.2.10 Wireless LAN

Wireless LAN specification is required to enable mobile users connecting to a LAN through a wireless (radio) connection. It provides the features and benefits of traditional LAN technologies such as Ethernet and Token Ring without the limitations of wires or cables. By using wireless LAN technology, users are able to Surf the web, to check e-mail or to take an online course without being confined to the work desk.

Recommended standard / specification:

- IEEE 802.11b – Institute of Electrical and Electronics Engineers Standard (IEEE) 802.11b.

IEEE 802.11b	
Description	802.11 is a family of specifications for wireless local area networks (Wireless LANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). There are currently five specifications in the family: 802.11a, 802.11b, 802.11e, 802.11g and 802.11h. All five use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing. 802.11a, 802.11b, and 802.11g are the three main specifications that define complete wireless LAN systems. 802.11e are

IEEE 802.11b	
	extensions to cater for QoS in 802.11 network. 802.11h attempts to add better control over transmission power and radio channel selection to 802.11a. IEEE 802.11b operates in the 2.4GHz frequency band. The main market opportunity for IEEE 802.11b is in the provision of wireless networking for small office/home office (SoHo) and home environments, or as a mechanism for providing wireless access at the fringes of the network in larger companies or in public areas, such as airport lounges and conference centres (where the technology has already been widely deployed). Already popular in the US, IEEE 802.11b is increasing in popularity in the rest of the world, especially since the cost of peripherals and infrastructure for the standard is falling rapidly.
Reference	IEEE 802.11b is one of the specifications in the IEEE 802.11 family of specifications for wireless LAN developed by IEEE. IEEE 802.11 specifications are available at http://standards.ieee.org/getieee802/802.11.html.
Rationale for Selection	▪ IEEE 802.11b is a *de facto* standard for Wireless LAN. ▪ IEEE 802.11 b is the most widely available and implemented wireless LANs today. ▪ The specification was accepted by the IEEE in 1997. ▪ 802.11b compliant products are readily available now.
Limitation	▪ Poor ability to transfer voice or video data. ▪ Congestion in the 2.4GHz band is a potential drawback.

2.2.11 Mobile Device Internet Access

Mobile Device Internet Access protocol is required to support Internet-based access from mobile devices such as mobile phones. It enables mobile devices users to obtain access to Internet-based content provided by the Government and the Public Sector.

Recommended standard / specification:

- WAP v2.0 – Wireless Application Protocol version 2

WAP v2.0	
Description	WAP is the *de facto* world standard for presentation and delivery of wireless information to mobile devices. The WAP protocol is based on Internet technology like IP and XML and is published by the WAP Forum. Today, all major mobile equipment manufactures like Nokia and Ericsson support the WAP protocol. WAP defines a communications protocol as well as an application environment. In essence, it is a standardised technology for cross-platform, distributed computing. It is the *de facto* standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants (PDAs) and other wireless terminals.
Reference	WAP v2.0 is a standard developed by the WAP Forum (now known as Open Mobile Alliance - established by the consolidation of the WAP Forum and the Open Mobile Architecture Initiative). The specifications are available at http://www.wapforum.org/what/technical.htm.
Rationale for Selection	▪ WAP is the *de facto* standard for mobile devices internet access.

WAP v2.0	
	▪ WAP is a matured standard: WAP version 1.0 specification was approved in 1998. WAP version 1.2 was approved in November 1999. WAP v2.0, the latest revision of the WAP specifications, was released in August 2001 and approved in December 2001. ▪ WAP is backed by all the major players in the industry – infrastructure and handset vendors, systems integrators, software suppliers, operators and content developers, which has ensured market acceptance of WAP, and is driving operators to incorporate WAP services into their strategies and planning.
Limitation	No known limitation on use of this standard.

2.2.12 Intra-Government Remote Services Delivery Protocol

The intra-government remote service delivery protocol, which defines the protocol for remotely requesting application functionality exposed through an interface, will be used by an application to request execution of a service provided by another application. The participating applications are autonomous – the implementation of the service is independent of the exposed interface.

Recommended standard / specification:

- SOAP v1.2 – Simple Object Access Protocol version 1.2.

SOAP v1.2	
Description	SOAP provides the definition of an XML document for the exchange of information, based on a one-way message exchange between a sender and receiver. Applications can combine SOAP messages to provide more sophisticated interactions, including remote procedure calls (RPCs) and conversational document exchange. SOAP messages can be exchanged using a variety of protocols, including application layer protocols, such as HTTP and SMTP. SOAP does not define data semantics, message routing, reliable data transfer etc. In summary, SOAP provides an extensible framework for application-to-application integration, capable of supporting a variety of integration scenarios incorporating new and existing applications.
Reference	SOAP v1.2 is developed and defined by W3C in 3 parts: ▪ Part 0: Primer at http://www.w3.org/TR/soap12-part0/; ▪ Part 1: Messaging Framework at http://www.w3.org/TR/soap12-part1; and ▪ Part 2: Adjuncts at http://www.w3.org/TR/soap12-part2/.
Rationale for Selection	▪ SOAP is being developed by the W3C XML Protocol Working Group as part of the Web Services Activity. ▪ SOAP is one of the core technologies that underpins web services and has significant industry support for a broad range of infrastructure and application providers. ▪ SOAP v1.2 were published as W3C Working Drafts in December 2001 and officially became a W3C Recommendation in December 2002. ▪ SOAP has broad industry support from

SOAP v1.2	
	– Application server vendors, including IBM, BEA, Microsoft and Sun Microsystems; – Enterprise application integration vendors, including IBM, TIBCO and WebMethods; – Application development tool vendors, including IBM, Borland, BEA and Microsoft; – Application vendors, including SAP and Oracle; – Content management vendors, including Documentum and Vignette; – Enterprise portal vendors, including IBM Websphere, Epicentric, Plumtree and Sybase.
Limitation	No known limitation on use of this standard.

2.2.13 Intra-Government Remote Services Description Language

The intra-government remote service description language will be used to standardise the way that application services are described to enable a standardised approach to requesting remote services, in accordance with the intra-government remote service delivery protocol standard. The language will be used to describe the interface in terms of characteristics such as its name, a description of its purpose, input parameters and results.

Recommended standard / specification:

- WSDL v1.1 – Web Services Description Language version 1.1

WSDL v1.1	
Description	WSDL defines an XML grammar for describing services in terms of the messages they can exchange and the operations which they can perform. It also defines a common binding mechanism to associate data formats and protocols with messages and operations. Bindings for SOAP, HTTP GET/POST and MIME are layered on top of the core service definition framework.
Reference	WSDL v1.1 is developed and defined by W3C at http://www.w3.org/TR/wsdl.
Rationale for Selection	▪ WSDL is the basis of the work of the Web Services Description Working Group of the W3C's Web Services Activity. ▪ WSDL is one of the core technologies which underpins web services and has significant industry support from a broad range of infrastructure and application providers. ▪ Version 1.1 is the basis of the Web Services Description Working Group work. ▪ WSDL has broad industry support from – Application server vendors, including IBM, BEA, Microsoft and Sun Microsystems; – Enterprise application integration vendors, including IBM, TIBCO and WebMethods; – Application development tool vendors, including IBM, Borland, BEA and Microsoft; – Application vendors, including SAP and Oracle; – Content management vendors, including Documentum and Vignette; – Enterprise portal vendors, including IBM Websphere,

WSDL v1.1	
	Epicentric, Plumtree and Sybase.
Limitation	No known limitation on use of this standard.

2.2.14 Intra-Government Remote Services Request Registry

Standard on Intra-Government Remote Services Request Registry is required to define the format, schemas and request protocols to publish and locate descriptions of services described using the intra-government remote service description language.

Should there be a need to publish service descriptions offered by the Government to enable applications to locate them dynamically, they can be published to a centralised registry. An application which requires access to a service can "interrogate" the registry to identify the appropriate service, determine the location of the interface description and then request the service remotely using the remote service delivery protocol.

However, in the early stage of deployment in an eGovernment environment, the service descriptions are only referenced at programming time, rather than at run time. Under such circumstances it would be sufficient to publish the service descriptions such that application developers are able to search and retrieve the description of the service they want to interact with, for example in a file system or database repository accessible via a web page.

Recommended standard / specification:

- UDDI v3 – Universal Description, Discovery and Integration version 3.

UDDI v3	
Description	UDDI defines information formats, schemas and request protocols to enable service requesters to dynamically discover or locate web services at runtime. A UDDI Business Registry – an implementation of the UDDI specifications – contains information about: ▪ Businesses, including name, description, contact information, industry category and references to more information ▪ Business services offered by a business – description, service category, references to information about the services ▪ Specification pointers – references to specifications and technical information about services ▪ Service types – pointers to technical specifications, such as interface definitions, message formats, message protocols and security protocols. Service interfaces can be described using WSDL and invoked using SOAP. The UDDI business registry can be accessed through both a browser-based interface and programmatically, via SOAP. Publicly accessible Business Registries are currently hosted by Microsoft, IBM, SAP and HP. In January 2002, NTT announced its intention to host a Business Registry. UDDI can also be deployed 'behind the firewall' e.g. for testing, cataloguing of internal web services and discovery of web services, behind the firewall.
Reference	UDDI is developed and defined by OASIS. Version 3 specification is published at http://uddi.org/pubs/uddi_v3.htm.
Rationale for	▪ UDDI is one of the core technologies which underpins web

UDDI v3	
Selection	services and has significant industry support from a broad range of infrastructure and application providers. ▪ Version 1 of the UDDI specification was published in September 2000. Version 2 was published in June 2001. UDDI version 3 Specification, Open Draft was published in July 2002. ▪ Publicly accessible UDDI business repositories: hosted by Hewlett ▪ Packard, IBM, Microsoft and SAP. NTT announced, in January 2002, its intention to host a UDDI repository. ▪ Directory servers: Sun Microsystems and Novell have announced plans to support UDDI with their directory products by 2002. ▪ Application servers: IBM supports UDDI with its WebSphere UDDI Registry.
Limitation	No known limitation on use of this standard.

3. RECOMMENDATIONS FOR DATA INTEGRATION

3.1 Overview

Data Integration covers components and technical specifications required to enable the recognition of data, including codes, recognition methods and interpretation (including formats used).

Interoperability components covered in the Data Integration area include:

- Default Document / Message Formatting Language;
- Default Schema Definition;
- Data Transformation;
- Data Modelling;
- Data Resource Description; and
- Minimum Interoperable Character Set.

3.2 Recommended Standards / Specifications

3.2.1 Default Document / Message Formatting Language

The Default Document / Message Formatting Language is to be used to define the format of data message and business documents, e.g. invoices and purchase orders, to be interchanged in between related parties such as Government agencies and departments as well as third parties e.g. suppliers.

Recommended standard / specification:

- XML v1.0 – Extensible Markup Language version 1.0 (Second Edition).

XML v1.0 (Second Edition)	
Description	XML is a markup language for documents containing structured information. It is a W3C Recommendation for marking up data that cannot be marked up using the HTML. It is a simple dialect of the Standard Generalized Markup Language (SGML) defined in ISO Standard 8879. The goal of XML is to enable SGML-coded data to be served, received, and processed on the Web in the way that is as easy as that currently made possible by the use of the fixed SGML tag set provided by HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML. XML is based on the ISO 10646 Universal Multiple-Octet Coded Character Set (UCS) so that it can be used in all major trading nations.
Reference	XML v1.0 (Second Edition) is a W3C Recommendation. The specification is published at http://www.w3.org/TR/REC-xml.
Rationale for Selection	▪ XML is a global, matured and widely adopted standard on data integration. ▪ XML is extensively supported by a broad range of application development, software infrastructure, business application and industry-specific schema initiatives. ▪ XML v1.0 was approved as a W3C Recommendation in February 1998. Second Edition was published as a W3C Recommendation in October 2000 which is not a new version of XML but merely incorporates the changes dictated by the first-edition errata as a convenience to readers.
Limitation	No known limitation on use of this standard.

3.2.2 Default Schema Definition

The Default Schema Definition is a language for defining schemas in XML messages/documents.

Recommended standard / specification:

- XML Schema v1.0 – XML Schema version 1.0.

XML Schema v1.0	
Description	XML Schema defines the structure, content and semantics of XML documents. It is appropriate for data-oriented message exchange and processing.
Reference	XML Schema v1.0 is a W3C Recommendation defined in 3 parts: ▪ Part 0: Primer at http://www.w3.org/TR/xmlschema-0/; ▪ Part 1: Structures at http://www.w3.org/TR/xmlschema-1/; and ▪ Part 2: Datatypes at http://www.w3.org/TR/xmlschema-2/.
Rationale for Selection	▪ XML Schema was approved as a W3C Recommendation on 2 May 2001. Version 1.0 is the current specification. ▪ Extensively supported by application development tools, application server, enterprise application integration, content management and business application products.
Limitation	No known limitation on use of this standard.

3.2.3 Data Transformation

Specification on Data Transformation enables dynamic filtering, conversion and reformatting of content to restructure and control how XML content is presented. For example, to transform a document formatted in accordance with a standard schema for delivery to another application.

Recommended standard / specification:

- XSL v1.0 – Extensible Stylesheet Language version 1.0.

XSL v1.0	
Description	XSL is a language for expressing stylesheets. It consists of two parts: ▪ a language for transforming XML documents, and ▪ an XML vocabulary for specifying formatting semantics. An XSL stylesheet specifies the presentation of a class of XML documents by describing how an instance of the class is transformed into an XML document that uses the formatting vocabulary.
Reference	XSL is a W3C Recommendation defined at http://www.w3c.org/TR/xsl and consists of 2 parts: ▪ XSL Translation (XSLT) at http://www.w3c.org/TR/xslt; and ▪ XML Path Language (XPath) at http://www.w3c.org/TR/xpath.
Rationale for Selection	▪ XSL is a W3C Standard. It became W3C recommendation in October 2001. XSLT and XPath became W3C recommendation in November 1999. ▪ XSL v1.0 (comprising XSLT and XPath) is widely supported by enterprise application integration, application server,

XSL v1.0	
	application development and content management products.
Limitation	No known limitation on use of this standard.

3.2.4 Data Modelling

Data Modelling standard is required to define the convention to be used for the interchange of system and data models among all the related parties, e.g. agencies, departments and third parties. This convention presents the conceptual design mainly for human interpretation.

Recommended standa rd / specification:

- UML v1.5 – Unified Modelling Language version 1.5.

UML v1.5	
Description	UML is an industry standard language for visualising, specifying, constructing and documenting data and systems which has been accepted by the Object Management Group (OMG). UML offers a standard way to write a system's blueprints, including conceptual things such as business processes and system functions as well as concrete things such as programming language statements, database schemas, and reusable software components.
Reference	UML is defined by OMG at http://www.omg.org/technology/documents/formal/uml.htm.
Rationale for Selection	▪ UML is a matured standard – it was accepted by the OMG in November 1997.

UML v1.5	
	▪ UML is supported by a broad range of application development, enterprise application integration, CASE, application server and software testing products for visualising, specifying, constructing and documenting data and systems. ▪ Version 1.5 is the current version.
Limitation	No known limitation on use of this standard.

3.2.5 Data Resource Description

In order to facilitate information sharing and retrieval, it is necessary to have standard descriptions e.g. author, subject, keywords etc., to avoid ambiguity in describing resources. Content/data resource description language will be referred to when defining documents, business specific schemas etc. to ensure consistent understanding and terminology. Standard on Data Resource Description is required to enable applications to exchange metadata and can be used in a variety of application scenarios e.g. to provide better search engine capabilities or in knowledge sharing and exchange. The standard does not define the metadata but instead defines the language which is used to represent that metadata.

Some governments have started to use this approach to manage their web content e.g. the UK Government has taken the lead to define an e-Government Metadata Standard (e-GMS) and Category List to help manage their information resources. Australia and New Zealand have implemented their Government Locator Services which are based on well described content.

In Malaysia, MAMPU has also adopted this approach by defining a Government Wide Data Dictionary to guide Government's agencies and departments to manage their information resources. A further detail on Government Wide Data Dictionary will be discussed in Section 6.

Recommended standard / specification:

- RDF – Resource Description Framework.

RDF	
Description	RDF data model defines a simple model for describing interrelationships among resources in terms of named properties and values. RDF properties may be thought of as attributes of resources and in this sense correspond to traditional attribute-value pairs. RDF properties also represent relationships between resources. As such, the RDF data model can therefore resemble an entity-relationship diagram. The RDF data model, however, provides no mechanism for declaring these properties, nor does it provide any mechanism for defining the relationships between these properties and other resources. The complete specification of the RDF consists of 5 components including RDF Model Theory, RDF/XML Syntax, RDF Schema, RDF Test Cases and RDF Primer.
Reference	RDF is a W3C framework defined at as defined by W3C at http://www.w3.org/TR/REC-rdf-syntax.
Rationale for Selection	▪ RDF is a W3C framework for supporting resource description or *metadata* (data about data), for the Web. RDF provides common structures that can be used for interoperable XML data exchange. ▪ RDF is a matured W3C Standard – RDF Model and Syntax

RDF	
	Specification was approved as a W3C Recommendation in September 2001.
Limitation	No known limitation on use of this standard.

3.2.6 Minimum Interoperable Character Set

Standard on Minimum Interoperable Character Set is required to define the minimum character sets to be used for the content to be interchanged in between related parties, e.g. agencies and departments as well as third parties such as suppliers.

Recommended standard / specification:

- UTF-8 – Universal Character Set (UCS) Transformation Format 8 Bit.

UTF-8	
Description	ISO/IEC 10646-1 defines a multi-octet character set called the Universal Character Set (UCS) which encompasses most of the world's writing systems. Multi-octet characters, however, are not compatible with many current applications and protocols, and this has led to the development of a few so-called UCS transformation formats (UTF), each with different characteristics. UTF-8 has the characteristic of preserving the full US-ASCII range, providing compatibility with file systems, parsers and other software that rely on US-ASCII values but are transparent to other values.
Reference	UTF-8 is a proposed IETF standard defined in RFC 2279 "UTF-8, a transformation format of ISO 10646".

UTF-8	
Rationale for Selection	▪ UTF-8 is a matured standard – an IETF standard since January 1998. It is widely supported by all dominant operating systems. ▪ UTF-8 preserves the full US-ASCII range, providing compatibility with file systems, parsers and software that rely on ASCII values.
Limitation	No known limitation on use of this standard.

4. RECOMMENDATIONS FOR INFORMATION ACCESS

4.1 Overview

Information Access covers components and technical specifications required to enable users to access Public Sector information and services electronically via a range of delivery channels (e.g. World Wide Web) and devices (e.g. personal computers, mobile phones, PDAs).

Interoperability components covered in the Information Access area include:

- Hypertext Web Content;
- Document;
- Spreadsheet;
- Presentation;
- Graphical Image;
- Moving Image and Audio / Visual;
- Audio / Video Streaming;
- Animation;
- Mobile Devices Content;
- Character Sets and Encoding;
- Compression; and
- Client-Side Scripting.

4.2 Recommended Standards / Specifications

4.2.1 Hypertext Web Content

Hypertext Web Content standards are required to specify the development and formatting of hypertext documents for presentation on browsers via a range of delivery channels including Internet and Intranet.

Recommended standards / specifications:

- HTML v4.01 – Hypertext Markup Language version 4.01; and
- XHTML v1.0 – Extensible Hypertext Markup Language version 1.0.

HTML v4.01	
Description	HTML is a simple markup language used to create hypertext documents that are platform independent. It is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user. HTML markup can represent hypertext news, mail, documentation, and hypermedia; menus of options; database query results; simple structured documents with in-lined graphics; and hypertext views of existing bodies of information.
Reference	HTML 4.01 specification is a W3C Recommendation and available at http://www.w3.org/TR/html401.
Rationale for Selection	▪ HTML is a global, matured and widely adopted standard. It has been in use by the World Wide Web (WWW) global information initiative since 1990. ▪ HTML v4.01 is the latest version of HTML. It was recommended by W3C in December 1999. ▪ It is widely supported by the dominant web browsers such as Microsoft Internet Explorer (IE), Netscape Navigator, Opera and Mozilla.
Limitation	The dominant browsers implement some features of HTML

HTML v4.01	
	v4.01 differently and provide non-standard extensions. It is strongly recommended that Government web content authors test the compatibility of their content with different combinations of popular browser configurations (including Netscape Navigator v4.7x or later, and Microsoft IE v5.x or later) and popular operating system configurations (including Microsoft Windows) and consult the appropriate vendor documentation which discusses restrictions and deviations from the specifications. Government web masters should also state on their web page how the content can best be viewed.

XHTML v1.0	
Description	W3C describes XHTML (eXtensible Hypertext Markup Language) as “a reformulation of HTML v4.0 as an application of the XML.” XHTML v1.0 reproduces and extends HTML v4 as XML and promises, with the advent of XHTML modularization, to simplify future extensions and to enable support for multiple devices. XHTML v1.0 was designed to enable easy migration of HTML content to XHTML and XML.
Reference	XHTML v1.0 specification is a W3C Recommendation and available at http://www.w3.org/TR/xhtml1.
Rationale for Selection	▪ XHTML is a matured and widely adopted standard. The latest version of XHTML (v1.0) was recommended by W3C in January 2000. ▪ It is widely supported by the dominant web browsers.

XHTML v1.0	
Limitation	No known limitation on use of this standard.

4.2.2 Document

Standards on Document are required to define the format and file types of documents for interchange between agencies and departments as well as third parties.

Recommended standards / specifications:

- Plain Text format (.txt) – for plain text and unformatted documents;
- Rich Text format (.rtf) version 1.6 – for documents interoperable across platforms;
- Portable Document format (.pdf) version 3, 4, 5 – for read-only documents; and
- Microsoft Word Document (.doc) – Word 97 format.

Plain Text Format (.txt)	
Description	Plain/unformatted text files.
Reference	N/A.
Rationale for Selection	It is the *de facto* standard for plain/unformatted text extensively supported by word processing packages, publishing tools, content management applications, e-mail applications etc.
Limitation	No known limitation on use of this standard.

Rich Text Format (.rtf) v1.6	
Description	The Rich Text Format (RTF) specification provides a format for text and graphics interchange that can be used with different

Rich Text Format (.rtf) v1.6	
	output devices, operating environments, and operating systems. RTF uses the American National Standards Institute (ANSI), PC-8, Macintosh, or IBM PC character set to control the representation and formatting of a document, both on the screen and in print. With the RTF specification, documents created under different operating systems and with different software applications can be transferred between those operating systems and applications.
Reference	RTF v1.6 specification is available at Microsoft Developer Network http://msdn.microsoft.com/library/?url=/library/en-us/dnrtfspec/html/rtfspec.asp?frame=true.
Rationale for Selection	▪ RTF is a *de facto* standard for text and graphics interchange, available in the public domain. ▪ RTF is matured and well supported by all of the market leading word processing packages. ▪ RTF version 1.6 is the latest version of the specification. It provides support for all new control words introduced by Microsoft Word for Windows 95 version 7.0, Word 97 for Windows, Word 98 for the Macintosh and Word 2000 for Windows and thus ensures maximum compatibility with the dominant word processing package.
Limitation	When documents are converted from a proprietary word processing format (e.g. .doc or .sxw) into RTF, features might be lost. In addition, different word processing software might render RTF documents in a slightly different way and some advanced features might not be supported, although in general the word processing software "understands the RTF format".

Rich Text Format (.rtf) v1.6	
	Hence there is no guarantee that the "look and feel" of a document can be preserved 100% when the document is created using one software package, exchanged as RTF, and rendered on the receiving end using different software or a different version of the same software.

Portable Document Format (.pdf) version 3, 4, 5	
Description	The Portable Document Format (PDF), developed by Adobe Systems Inc., is a computer file format designed to publish and distribute electronic documents. PDF is related to the Postscript language, and may be used with text, image, and/or multimedia files. PDF files may be created and used on most any type of computer e.g. Windows, Macintosh, UNIX, or OS/2. Unlike other electronic file formats such as HTML or XML, the PDF captures all of the elements of a printed document as an electronic image and preserves the exact layout, font attributes, and formatting of the document from which it was created, ensuring that the electronic version of a document appears just like the original. Users can view, navigate, print and forward to other users.
Reference	Acrobat PDF homepage at http://www.adobe.com/products/acrobat/adobepdf.html.
Rationale for Selection	▪ PDF is a dominant format for document publishing which is extensively used on the Internet. ▪ It is supported by freely available Acrobat Reader and browser plug-ins. ▪ PDF is a matured format i.e. Version 3.0 released 1996.

Portable Document Format (.pdf) version 3, 4, 5	
	Version 4.0 released early 1999. Version 5.0 released 2001. ▪ Access controls and permissions can be defined in PDF documents, so that only authorised people will be able to view, modify, repurpose, or even print documents.
Limitation	No known limitation on use of this standard.

Microsoft Word Document (.doc) – Word 97 format	
Description	.doc document file type is the proprietary Microsoft Word document format. This format is to be used in inter-departmental information interchange between users of Microsoft Word.
Reference	Microsoft Word homepage at http://www.microsoft.com/office/word/default.asp.
Rationale for Selection	▪ It is one of the major word processing applications both in public and private sector. ▪ It is supported by open source alternatives. ▪ Version Word 97 file format should be treated as the file format for exchange as later versions share the same file format due to its longer existence in the market (since year 1997) and supported by later version of Microsoft Word, e.g. Word 2000 and Word XP.
Limitation	Incompatibilities between Word 97 and other versions exist (due to newly introduced features).

4.2.3 Spreadsheet

Standards on Spreadsheet are required to define the format and file types of spreadsheets for interchange between agencies and departments as well as third parties.

Recommended standards / specifications:

- Comma Separated Variable/Delimited files format (.csv) – for spreadsheet interoperable across spreadsheet applications; and
- Microsoft Excel Spreadsheet (.xls) – Excel 97 format.

Comma Separated Variable / Delimted File Format (.csv)	
Description	.csv is the *de facto* standard for delimited files for use in interdepartmental information interchange.
Reference	N/A.
Rationale for Selection	▪ .csv is a matured and widely adopted file format for spreadsheet. ▪ It is extensively supported by dominant spreadsheet applications such as Microsoft Excel, Lotus 123, and OpenOffice Calc.
Limitation	No known limitation on use of this standard.

Microsoft Excel Spreadsheet (.xls)	
Description	.xls spreadsheet file type is the proprietary Microsoft Excel spreadsheet format. This format is to be used in inter-departmental information interchange between users of Microsoft Excel.

Microsoft Excel Spreadsheet (.xls)	
Reference	Microsoft Excel homepage at http://www.microsoft.com/office/excel/default.asp.
Rationale for Selection	▪ Microsoft Excel is one of the major spreadsheet applications both in public and private sector. ▪ It is supported by open source alternatives. ▪ Version Excel 97 file format should be treated as the file format for exchange as later versions share the same file format due to its longer existence in the market (since year 1997) and supported by later version of Microsoft Excel, e.g. Excel 2000 and Excel XP.
Limitation	The Excel 2000 file format is backwardly compatible with Excel 97. This means you do not have to do anything special to open or save workbooks from either of these versions. However, features unique to Excel 2000 may not be displayed the same way in Excel 97. For instance, a workbook that contains a PivotChart™ report created in Excel 2000 will display a PivotChart report in Excel 2000, but will display a regular chart sheet in Excel 97. Also, Visual Basic® for Applications macros that use commands new to Excel 2000 may result in compile errors when run in Excel 97.

4.2.4 Presentation

Standards on Presentation are required to define the format and file types of presentations for interchange between agencies and departments as well as third parties.

Recommended standards / specifications:

- Hypertext Document format (.htm) – for presentation interoperable across dominant browsers (refer to Section 4.2.1 for introduction on HTML v4.02);
- Portable Document format (.pdf) – for read-only presentation (refer to Section 4.2.2 for introduction on Portable Document format); and
- Microsoft PowerPoint Presentation (.ppt) – PowerPoint 97 format.

Microsoft PowerPoint Presentation (.ppt)	
Description	.ppt presentation file type is the proprietary Microsoft PowerPoint presentation format. This format is to be used in inter-departmental information interchange between users of Microsoft PowerPoint.
Reference	Microsoft PowerPoint homepage at http://www.microsoft.com/office/powerpoint/default.asp.
Rationale for Selection	▪ Microsoft PowerPoint is one of the major presentation applications both in public and private sector. ▪ It is supported by open source alternatives. ▪ Version PowerPoint 97 file format should be treated as the file format for exchange as later versions share the same file format due to its longer existence in the market (since year 1997) and supported by later version of Microsoft PowerPoint, e.g. PowerPoint 2000 and PowerPoint XP.
Limitation	Incompatibilities between PowerPoint 97 and other versions exist

Microsoft PowerPoint Presentation (.ppt)	
	(due to newly introduced features).

4.2.5 Graphical Image

Standards on Graphical Image are required to define the format and files types of graphics and still images for interchange between agencies and departments as well as third parties.

Recommended standards / specifications:

- Joint Photographic Experts Group (.jpg);
- Graphic Interchange Format (.gif) version 89a; and
- Tag Image File Format (.tif).

Joint Photographic Experts Group (.jpg)	
Description	Joint Photographic Experts Group (JPEG) is an ISO graphic image file format standard (ISO 10918).
Reference	JPEG standard is defined by ISO standard 10918.
Rationale for Selection	▪ JPEG standard is widely supported by browsers and the majority of image processing, graphics design, photo processing and scanner accessory software. ▪ It is a matured standard - originally ratified in 1994 and natively supported by Netscape Navigator and IE since version 2.
Limitation	No known limitation on use of this standard.

Graphic Interchange Format (.gif) version 89a	
Description	Graphic Interchange Format (GIF) is one of the most common formats for graphics images on the Web.
Reference	GIF v89a is a standard defined by CompuServe Incorporated and available at http://www.w3.org/Graphics/GIF/spec-gif89a.txt.
Rationale for Selection	▪ Graphic Interchange Format is a *de facto* standard widely supported by browsers and the majority of image processing, graphics design, photo processing and scanner accessory software. ▪ It is natively supported by IE since v3 and Netscape Navigator since v2. ▪ Version 89a is the latest version.
Limitation	No known limitation on use of this standard.

Tag Image File Format (.tif)	
Description	Tag Image File Format (TIFF) was developed by Aldus and Microsoft Corp, and the specification was owned by Aldus, which in turn merged with Adobe Systems, Incorporated. Consequently, Adobe Systems now holds the Copyright for the TIFF specification. TIFF is a common format for exchanging raster graphics (bitmap) images between application programs. It is a *de facto* standard of particular benefit for images that will not tolerate information loss.
Reference	TIFF version 6 specification is available at http://partners.adobe.com/asn/developer/pdfs/tn/TIFF6.pdf.

Tag Image File Format (.tif)	
Rationale for Selection	▪ TIFF is a *de facto* standard of particular benefit for images that will not tolerate information loss. ▪ Version 6 is the current version and a matured standard. It was published in June 1992. ▪ It is widely supported by browsers through freely-available plug-ins and the majority of image processing, graphics design, photo processing and scanner accessory software.
Limitation	No known limitation on use of this standard.

4.2.6 Moving Image and Audio / Visual Contents

Standards on Moving Image and Audio/Visual contents are required to define the compressed format and file types of audio/visual content such as movies, for interchange between agencies and departments as well as third parties.

Recommended standard / specification:

- MPEG-1 – Moving Picture Experts Group.

MPEG-1	
Description	The MPEG standards are an evolving set of standards for video and audio compression and for multimedia delivery developed by the Moving Picture Experts Group (MPEG). MPEG-1 was designed for coding progressive video at a transmission rate of about 1.5 million bits per second.
Reference	MPEG-1 is defined by ISO Standard 11172.

MPEG-1	
Rationale for Selection	▪ MPEG-1 is a global, matured and widely adopted standard. It was approved in 1992. ▪ It is an ISO standard for compression, decompression, processing and coded representation of moving pictures, audio and their combination. ▪ It is the dominant standard for audio and video on the Internet. MPEG players are freely available. Conversion is provided by most mainstream packages.
Limitation	No known limitation on use of this standard.

4.2.7 Audio/Video Streaming

Standards on Audio/Video Streaming are required to define the formats and file types streaming audio/video content such as web casts and web seminars, for interchange between agencies and departments as well as third parties.

Recommended standards / specifications:

- Microsoft Windows Media Player (.asf, .wma, .wmv); and
- Real Audio / Real Video (.ra, .ram, .rm, .rmm).

Microsoft Windows Media Player (.asf, .wma, .wmv)	
Description	Microsoft WMP is a proprietary format from Microsoft for receiving streamed content in real time.
Reference	Microsoft WMP homepage at http://www.microsoft.com/windows/windowsmedia/.
Rationale for Selection	▪ Microsoft WMP is a commonly used format for audio/video streaming on the Web, with freely available players.

Microsoft Windows Media Player (.asf, .wma, .wmv)	
	▪ No specific version need be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitation	No known limitation on use of this standard. However, the webmaster should be aware that the later versions of free viewers are not supported on Win95 and NT4.

Real Audio / Real Video (.ra, .ram, .rm, .rmm)	
Description	Real Audio / Real Video is a proprietary format from Real Networks for receiving streamed content in real time.
Reference	Real Audio / Real Video documentation homepage at http://www.realnetworks.com/resources/documentation/.
Rationale for Selection	▪ Real Audio / Video is one of the most commonly used formats for continuous streaming of audio and video with browser plug-ins and players freely available. ▪ No specific version need to be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitation	No known limitation on use of this standard.

4.2.8 Animation

Animation standards are required to define the applications and formats to be used for the interchange of animated content between agencies and departments as well as third parties.

Recommended standards / specifications:

- Macromedia Flash (.swf);
- Macromedia Shockwave (.swf); and
- Apple Quicktime (.avi, .mov, .qt).

Macromedia Flash (.swf)	
Description	The Macromedia Flash file format (.swf) delivers vector graphics and animation over the Internet to the Macromedia Flash Player. Flash, a popular authoring software developed by Macromedia, is used to create animation programs with full-screen navigation interfaces, graphic illustrations, and simple interactivity in resizable file format that is small enough to stream across a normal modem connection.
Reference	Macromedia Flash file format specification is defined by Macromedia and published at http://www.macromedia.com/software/flash/open/licensing/fileformat/.
Rationale for Selection	▪ It is a very commonly used format for animation on the Web, with freely available players and browser plug-ins. ▪ No specific version needs to be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitation	No known limitation on use of this standard.

Macromedia Shockwave (.swf)	
Description	The Shockwave Player displays Web content that has been created by Macromedia Director Shockwave Studio.

Macromedia Shockwave (.swf)	
Reference	Macromedia Shockwave homepage at http://www.macromedia.com.
Rationale for Selection	▪ It is a very commonly used format for animation on the Web, with freely available players and browser plug-ins. Players are freely available for Apple and Microsoft operating systems. ▪ No specific version needs to be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitation	No known limitation on use of this standard.

Apple Quicktime (.avi, .mov, .qt)	
Description	Quicktime is a multimedia development, storage, and playback technology from Apple, Inc.. Quicktime files combine sound, text, animation, and video in a single file.
Reference	Quicktime file format specification is defined by Apple, Inc. and published at http://www.apple.com/quicktime/products/qt/specifications.html.
Rationale for Selection	▪ It is a very commonly used format for animation on the Web, with freely available players and browser plug-ins. Players are freely available for Apple and Microsoft operating systems. ▪ No specific version needs to be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitation	No known limitation on use of this standard.

4.2.9 Mobile Devices Content

Standard on Mobile Device Content is required to define the format of content for presentation on mobile devices such as mobile phone and PDAs.

Recommended standard / specification:

- WML v2.0 – Wireless Markup Language version 2.0.

WML v2.0	
Description	WML is a language that allows the text portions of Web pages to be presented on mobile telephones and PDAs via wireless access. WML is part of the Wireless Application Protocol (WAP).
Reference	WML v2.0 is a standard (part of WAP v2.0 specification) developed by the WAP Forum (now known as Open Mobile Alliance - established by the consolidation of the WAP Forum and the Open Mobile Architecture Initiative). The specifications are available at http://www.wapforum.org/what/technical.htm.
Rationale for Selection	▪ WML is a globally recognized and matured standard. WML version 1.0 was introduced in 1998. Since this date several updates have been made. WML v1.2 was approved by the WAP Forum in November 1999. WML v2.0 was released and approved in August 2001. ▪ WML has become the standard mark-up language for the development of content for small screen wireless devices based on WAP (and is thus compatible with mobile network standards such as GSM, CDMA, TDMA and packet-switched data standards such as GPRS, IS95B and 3G). ▪ Version 2.0 is the latest version of WML and it is supported by microbrowsers from the leading microbrowser vendors

WML v2.0	
	such as Openwave, Microsoft, and Nokia.
Limitation	No known limitation on use of this standard.

4.2.10 Character Sets and Encoding

Character Sets and Encoding standards define the character sets to be used for content to be interchanged in English or Malay, as well as how those characters are to be encoded.

Recommended standards / specifications:

- ASCII – American Standard Code for Information Interchange;
- ISO/IEC 10646-1:2000 (revision of ISO 10646);
- UTF-16 – Universal Character Set (UCS) Transformation Format 16 Bit; and
- UNICODE version 3.

ASCII	
Description	ASCII is a character set and a character encoding based on the Roman alphabet as used in modern English. It is most commonly used by computers and other communication equipment to represent text and by control devices that work with text.
Reference	ASCII was developed by developed by the American National Standards Institute (ANSI) and is defined in ISO Standard 646.
Rationale for Selection	▪ ASCII is the dominant standard for coding textual content in English. ▪ ASCII is an extremely matured standard. It was first published as ANSI X3.4 in 1968.

ASCII	
Limitation	No known limitation on use of this standard.

ISO/IEC 10646-1:2000	
Description	ISO 10646 is an ISO standard to encode the characters of the major languages of the world into a single character set. ISO 10646 is code-for-code compatible with Unicode which can be considered as an implementation of 10646. Unicode can be encoded in different ways. Data messages (e.g. XML messages) encoded in Unicode should adopt UTF-8 as the encoding standard unless the Government specifies otherwise.
Reference	ISO10646-1:2000 is a ISO Standard, a revision of ISO 10646.
Rationale for Selection	▪ ISO 10646 is a global and matured standard. First published in 1993. Latest 2 revisions are ISO 10646-1:2000 (generally referred as extension A) and ISO 10646-2:2001 (generally referred as extension B). ▪ It is widely supported by a broad range of products, including databases, fonts and printing tools, internationalisation libraries and office productivity tools. ▪ Version ISO 10646-1:2000 is to be adopted because product support for ISO 10646-2:2001 is immature.
Limitation	No known limitation on use of this standard.

UTF-16	
Description	The Unicode Standard [UNICODE] and ISO/IEC 10646 [ISO-10646] jointly define a coded character set (CCS), hereafter referred to as Unicode, which encompasses most of the world's writing systems. UTF-16, the object of this specification, is one of the standard ways of encoding Unicode character data; it has the characteristics of encoding all currently defined characters (in plane 0, the BMP) in exactly two octets and of being able to encode all other characters likely to be defined (the next 16 planes) in exactly four octets.
Reference	UTF-16 is a IETF proposed standard and defined by RFC 2781 "UTF-16, an encoding of ISO 10646".
Rationale for Selection	UTF-16 is a global, matured and widely adopted standard for character set.
Limitation	UTF-16 is based on the ISO 10646 character set, which is frequently being added to, as described in Section 6 and Appendix A of this document. Processors must be able to handle characters that are not defined at the time that the processor was created in such a way as to not allow an attacker to harm a recipient by including unknown characters.

UNICODE v3.0	
Description	The Unicode Standard is the universal character encoding scheme for written characters and text. It defines a consistent way of encoding multilingual text that enables the exchange of

UNICODE v3.0	
	text data internationally and creates the foundation for global software. As the default encoding of HTML and XML, the Unicode Standard provides a sound underpinning for the World Wide Web and new methods of business in a networked world. Required in new Internet protocols and implemented in all modern operating systems and computer languages such as Java, Unicode is the basis of software that must function all around the world.
Reference	UNICODE v3.0 is defined by Unicode Consortium at http://www.unicode.org/book/u2.html.
Rationale for Selection	Unicode v3.0 is a global, matured and widely adopted standard for character set.
Limitation	No known limitation on use of this standard.

4.2.11 Compression

Compression standards are required to define the applications and format to be used for compressing files for interchange in between related parties.

Recommended standards / specifications:

- Zip (.zip); and
- GNU Zip (.gz) version 4.3.

Zip (.zip)	
Description	Files in a zip file are compressed so that they take up less space in storage or take less time to send to someone.

Zip (.zip)	
Reference	Zip specification is available at http://www.pkware.com/products/enterprise/white_papers/appnote.htm.
Rationale for Selection	▪ Zip is the *de facto* standard for file compression. ▪ It is a global, matured and widely adopted standard. It was introduced in 1989. ▪ It is supported on a range of operating systems including DOS, Windows and UNIX. Extractors are freely available eg PKZip, WinZip for private use. Corporate licences for these tools are also available.
Limitation	No known limitation on use of this standard.

GNU Zip (.gz) v4.3	
Description	GZIP (GNU zip) is a compression utility. It has been adopted by the GNU project and is popular on the Internet.
Reference	GZIP is an IETF standard defined by RFC 1952 "GZIP file format specification version 4.3".
Rationale for Selection	▪ GZIP is a commonly utilised file compression format. ▪ Version 4.3 is the current version and is documented in RFC 1952. ▪ It is supported on a range of operating systems including DOS, UNIX and MacOS. It can be extracted on Windows operating systems using the freely available WinZip utility.
Limitation	No known limitation on use of this standard.

4.2.12 Client-Side Scripting

Client-side scripts are programs written and attached or embedded to HTML documents in a manner independent of the scripting language. The scripts add interactivity and program logic to browser-based content, for instance, provide run-time validation of form field contents by responding to a user's mouse action with the execution of program to validate user input. It reduces server load by transferring some of the processing of the program to be handled locally at client.

Standard on client-side scripting is required to ensure consistency on the scripts implementation at different browsers, in particular, the dominant browsers such as Microsoft IE and Netscape Navigator.

Recommended standard / specification:

- ECMA 262 – ECMA 262 Script 3rd Edition

ECMA 262 Script 3rd Edition	
Description	ECMA Script is a standard scripting language developed with the co-operation of Netscape and Microsoft based on several originating technologies e.g. JavaScript (Netscape) and JScript (Microsoft). The language was invented by Netscape and first appeared in that Netscape Navigator 2.0 browser. It has appeared in all subsequent browsers from Netscape and in all browsers from Microsoft starting with IE 3.0. Having ECMAScript standard will help to ensure more consistency between the dominant browsers, i.e. Netscape Navigator and Microsoft IE, and other Web script

ECMA 262 Script 3 rd Edition	
	implementations.
Reference	ECMA 262 Script 3rd Edition is defined in ECMAScript Language Specification and adopted by ECMA General Assembly. The specification is available at http://www.ecma-international.org/.
Rationale for Selection	▪ ECMA 262 is a well-recognised industry standard with support by the dominant browsers such as IE, Netscape Navigator, and Opera. ▪ 3rd Edition is the current version released in 1999 and is supported by the dominant browsers, i.e. IE 5.x or later, Netscape Navigator 4.5 or later, and Opera 4.02 or later . ▪ There are no alternative standards.
Limitation	Not all browsers support client-side scripting even though the dominant browsers such as IE and Netscape support it. Government web content authors should test compatibility of their client-side scripts with different browsers as well as different versions of browsers to ensure their scripts are compatible, especially with browser versions that are being used by the public.

5. RECOMMENDATIONS FOR SECURITY

5.1 Overview

Security covers components and technical specifications needed to enable the secure exchange of information as well as the secure access to the Public Sector information and services.

Interoperability components covered in the Security area include:

- Email Security;
- Transport Level Security;
- Network Level Security;
- Network Level Encryption;
- Encryption Algorithms;
- Digital Signature Algorithms;
- Hashing Algorithms for Digital Signatures;
- Key Transport Algorithms;
- XML Message Encryption;
- XML Message Signature; and
- Privacy Policy.

5.2 Recommended Standards / Specifications

5.2.1 Email Security

Email security standard is required to support the security of email messages, in particular, messages which may include authenticity, integrity and confidentiality. Email products must support interfaces that conform to the email security standards for sending secure messages.

Recommended standard / specification:

- S/MIME v3 – Secure Multi-purpose Internet Mail Extensions version 3

S/MIME v3	
Description	S/MIME provides a method to send and receive secure MIME messages by sending e-mail that uses the Rivest-Shamir-Adleman (RSA) encryption system. S/MIME is included in the latest versions of the email clients from Microsoft and Netscape and has also been endorsed by other vendors that make messaging products.
Reference	S/MIME is a proposed IETF standard defined in: ▪ RFC 2630 "Cryptographic Message Syntax"; ▪ RFC 2631 "Diffie-Hellman Key Agreement Method"; ▪ RFC 2632 "S/MIME Version 3 Certificate Handling"; and ▪ RFC 2633 "S/MIME Version 3 Message Specification".
Rationale for Selection	▪ S/MIME is a matured standard. Version 3 is the latest version and it was made an IETF standard in July 1999. ▪ S/MIME is a well supported standard and has been selected over the alternatives such as PGP (not suited to large user communities), PEM and MIME Object Security services (neither of these standards has gained significant industry support). ▪ S/MIME v3.0 is widely supported by the latest versions of the market leading email products such as Microsoft, Netscape and IBM.
Limitation	No known limitation on use of this standard.

5.2.2 Transport Level Security

Security standards on Transport Level are required to support transport level security that enables authentication of clients and servers as well as encryption of data when using TCP/IP -based protocols such as HTTP.

Recommended standards / specifications:

- SSL v3.0 – Secure Sockets Layer version 3.0; and
- TLS v1.0 – Transport Layer Security version 1.0.

SSL v3.0	
Description	SSL is a commonly used protocol for managing the security of a message transmission on the Internet. SSL was developed by Netscape with its major goal is to provide privacy and reliability between two communicating applications, and prevents eavesdropping, tampering or message forgery. The SSL protocol runs above TCP/IP and bellow higher-level protocols such as TELNET, FTP or HTTP. It provides for encryption, server and client authentication and message authentication.
Reference	SSL v3.0 is developed and defined by Netscape at http://wp.netscape.com/eng/ssl3/.
Rationale for Selection	▪ SSL is a matured standard – Netscape final draft specification released in November 1996 and the IETF TLS Working Group began working with SSL v3.0 in 1996. ▪ SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by

SSL v3.0	
	Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the *de facto* standard until evolving into Transport Layer Security (TLS). ▪ SSL v3.0 is the latest version of SSL and available in most dominant browsers with either 40 bit or 128-bit encryption.
Limitation	No known limitation on use of this standard.

TLS v1.0	
Description	TLS has been proposed as the successor to SSL. The differences between TLS v1.0 and SSL v3.0 are not dramatic, but they are significant enough that TLS v1.0 and SSL v3.0 do not communicate directly. Instead, if a TLS v1.0 client encounters an SSL v3.0 server or vice versa it reverts to SSL v3.0, allow ing the two to coexist. The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications. The IETF has published two RFCs describing the use of the upgrade mechanism in HTTP/1.1 to initiate TLS (RFC 2817) and how to use HTTP over TLS (RFC 2246).
Reference	TLS is a proposed IETF standard defined in RFC 2246 “The TLS Protocol Version 1.0”.
Rationale for Selection	▪ TLS is a proposed IETF standard, RFC 2246, and is thus deemed to be generally stable, has resolved known design choices, is believed to be well-understood, has received

TLS v1.0	
	significant community review, and appears to enjoy enough community interest to be considered valuable. ▪ TLS is a matured standard - TLS version 1.0 is outlined in the IETF's RFC 2246 dated January 1999. ▪ TLS v1.0 is virtually universally available with support by the market leading browsers, including Netscape Navigator and IE and web servers, including Apache, Microsoft IIS and iPlanet.
Limitation	Early versions of web server software exhibited interoperability problems between TLS v1.0 and SSL v3.0. Agencies and departments should seek confirmation from vendors that such problems do not exist with the version of web server software deployed and, if they do, appropriate action should be taken to rectify the problems.

5.2.3 Network Level Security

Network Level Security standard is required to provide security at network level. It is to be used for implementation of Virtual Private Networks (VPNs) and secure remote access, as well as provision for authentication of the originating computer.

Recommended standard / specification:

- IPsec – Internet Protocol Security.

IPsec	
Description	IPsec is a general mechanism for securing IP. It is a standard for security at the network or packet processing layer of network communication. It builds security into the fabric of the Internet so that anyone who choses to communicate securely can do so, as easily as they can do anything else on the net. There are two protocols used in an IPsec implementation: ▪ ESP, Encapsulating Security Payload, – Encrypts and/or authenticates data; ▪ AH, Authentication Header, – Provides a packet authentication service.
Reference	IPsec is a proposed IETF standard defined in: ▪ RFC 2402 “IP Authentication Header”; and ▪ RFC 2404 “The Use of HMAC-SHA-1-96 within ESP and AH”.
Rationale for Selection	▪ IPsec is the only viable standard for IP network-level security. Over the last couple of years, IPsec has grown to be the preferred choice for providing secure VPN communications over the public Internet, and with the integration of IPsec support within Windows 2000, it is likely to become a dominant standard. ▪ IPsec is widely adopted by all IP VPN products, for example, those provided by market leaders such as IBM, Cisco Systems IOS and Checkpoint Software.
Limitation	The Internet is running under IPv4 which has numerous shortcomings of which the shortage of IP addresses is the most pressing. IPv6 has been proposed with much longer addresses to

IPsec	
	remedy these problems but its adoption is almost stalled by the enormous inertia of the installed base of IPv4. The shortage of addresses, aggravated by the biased allocation of them (most are reserved for organisations in the USA) has led to various dynamic address sharing tricks. These prevent the full implementation of the IPsec protocols, and have given rise to various potential security vulnerabilities (when an address is assigned to a different person). IPv6 provides the functionality that is today found in IP VPN products.

5.2.4 Network Level Encryption

Standard on Network Level Encryption is required to support the encryption at network level. It adds support for encryption of data in addition to the authentication of the originating computer provided by network level security.

Recommended standard / specification:

- IP ESP – IP Encapsulating Security Payload.

IP ESP	
Description	IP ESP provides confidentiality, data origin authentication, connectionless integrity, anti-replay services and traffic flow confidentiality with IPv4 and IPv6 networks. ESP may be applied alone, in combination with the IP Authentication Header (AH), or in a nested fashion, e.g., through the use of tunnel mode.
Reference	IP ESP is a proposed IETF standard defined in RFC 2406 “IP

IP ESP	
	Encapsulating Security Payload (ESP)".
Rationale for Selection	▪ IP ESP is the only viable standard for IP network-level encryption and is an IETF standard. ▪ IP ESP is a matured standard. It was a proposed IETF standard since 1998. ▪ IP ESP is widely used in VPN products which are supplied by numerous vendors, including all of the leading firewall vendors such as IBM, Cisco, Computer Associates, HP, and Symantec.
Limitation	No known limitation on use of this standard.

5.2.5 Encryption Algorithms

Standards on Encryption Algorithms are required to ensure confidentiality and security of information in the process of information exchange in particular dealing with Government information resources.

Recommended standards / specifications:

- Data Encryption Standard (DES); and
- Triple Data Encryption Standard (3DES).

Data Encryption Standard (DES)	
Description	DES is a widely used method of data encryption using a private (secret) key that was judged so difficult to break by the US government that it was restricted for exportation to other countries until January 2000. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be

Data Encryption Standard (DES)	
	used. For each given message, the key is chosen at random from among this enormous number of keys. Both the sender and the receiver must know and use the same private key. DES supports a key length of 56 bits.
Reference	DES was originated at IBM in 1977 and was adopted by the U.S. Department of Defense. It is specified in the ▪ ANSI X3.92 and X3.106 standards; and ▪ Federal FIPS 46-3 and 81 standards.
Rationale for Selection	▪ DES is very widely used and highly matured – it was developed based on Lucifer standard from IBM Research in 1977. ▪ It is currently the basis of SSL encryption. ▪ DES (and 3DES) are the most widely used encryption standards supported by the majority of products which require encryption.
Limitation	No known limitation on use of this standard.

Triple Data Encryption Standard (3DES)	
Description	3DES is a stronger version of DES, as the encrypted communication is re-encrypted twice to make it harder to crack. It is still a relatively efficient encryption algorithm. It belongs to the “symmetric” family of algorithms (i.e. both parties to a communication have to be in possession of the same secret key before 3DES starts). This can be done by one party generating a random key and sending it to the other party using public key (RSA) cryptography.

Triple Data Encryption Standard (3DES)	
	3DES supports a key length of 168 bits.
Reference	3DES is defined by FIPS 46-3 and ANS X9.52-1998.
Rationale for Selection	▪ 3DES is a stronger version of DES and is a FIPS (46-3)and ANSI approved standard (ANSI X9.52-1998). ▪ The 3DES variant of DES is now widely used to enhance security. ▪ 3DES (and DES) are the most widely used encryption standards supported by the majority of products which require encryption.
Limitation	No known limitation on use of this standard.

5.2.6 Digital Signature Algorithms

Digital Signature Algorithms standards are required for the generation of public and private keys for use with public key infrastructure (PKI) and to provide authentication through digital signatures.

Recommended standards / specifications:

- DSA – Digital Signature Algorithm; and
- RSA for Digital Signature.

Digital Signature Algorithm (DSA)	
Description	NIST published the DSA in the Digital Signature Standard (DSS), which is a part of the U.S. government's Capstone project. DSS was selected by NIST, in co-operation with the NSA to be the digital authentication standard of the US Government. The standard was issued in May 1994. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. The DSA provides the capability to generate and verify signatures. NIST defines key sizes of 512-1024 bits.
Reference	DSA is defined by NIST in FIPS 186-2 DSS.
Rationale for Selection	▪ Together with RSA, DSA is a widely accepted standard for digital signature algorithms. ▪ It is a matured standard – issued in 1994.
Limitation	No known limitation on use of this standard.

Rivest-Shamir-Adleman (RSA) for Digital Signatures	
Description	RSA for Digital Signatures is an alternative method for generating and checking digital signatures. It is recognised by the NIST within the DSS as an alternative to DSA. RSA is a proprietary public-key cryptography system, from

Rivest-Shamir-Adleman (RSA) for Digital Signatures	
	RSA Security, that provides both encryption and digital signatures. RSA uses the public key of the recipient to encrypt data which can only be decrypted by the recipient using their private key. RSA supports key lengths of 512-2048 bits. RSA recommends 768-bit keys for less valuable data, 1024-bit keys for corporate use and 2048-bit keys for extremely valuable data.
Reference	RSA for Digital Signature is recognised in FIPS 186-2 DSS as an alternative to DSA.
Rationale for Selection	▪ RSA is a matured security standard – it was first developed in 1997 and has been extensively tested. ▪ RSA for Digital Signature is a proprietary standard introduced in February 2000, which has gained wide acceptance. ▪ RSA is the most widely used digital signature algorithm. It has been licensed to 700 companies and RSA claims an installed base of more than 500 million.
Limitation	No known limitation on use of this standard.

5.2.7 Hashing Algorithms for Digital Signatures

Standard on hashing algorithms for digital signatures is required for digital signature implementations. Hashing algorithms take a message and produce a message digest which is used to verify the integrity of a message for use with digital signatures.

Recommended standard / specification:

- SHA-1 – Secure Hash Algorithms 1.

SHA-1	
Description	SHA-1 is a message digest algorithm (and cryptographic hash function) designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST). It produces a 160-bit digest from a message with a maximum size of 2^64 bits. The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. The NIST has published three additional variants of SHA, each with longer digests. These are named after their digest lengths (in bits): SHA-256, SHA-384, and SHA-512. They were first published in 2001 in the draft FIPS PUB 180-2, at which time review and comment were accepted. FIPS PUB 180-2, which also includes SHA-1, was released as an official standard in 2002. These new hash functions have not yet received as much scrutiny by the public cryptographic community as SHA-1 has, and so their cryptographic security is not yet as assured. FIPS PUB 180-1 also encouraged the adoption and use of SHA-1 by private and commercial organizations.
Reference	SHA-1 is a NIST approved standard defined in FIPS 180-1 “Secure Hash Standard” as well as a proposed IETF standard

SHA-1	
	defined in RFC 3174 “US Secure Hash Algorithm 1 (SHA1)”.
Rationale for Selection	▪ NIST has approved hash algorithm SHA-1 for digital signatures. ▪ SHA-1 is a matured standard - original specification of the algorithm (SHA-0) was published in 1993 and the revised version (SHA-1) was published in 1995. ▪ SHA-1 has been very closely examined by the public cryptographic community and no cryptographic insecurities have yet been found. It is therefore considered to be quite secured.
Limitation	No known limitation on use of this standard.

5.2.8 Key Transport Algorithms

Key transport algorithms are the encryption algorithms specified for encrypting and decrypting keys. There algorithms are key establishment methods by which a secret key is generated by one entity in a communication association and securely sent to another entity in the association. For example, a message originator can generate a random session key and then use the key transport algorithm to encrypt that key with the public key of the intended recipient.

Recommended standards / specifications:

- Digital Signature Algorithm (DSA) (refer to Section 5.2.6 for introduction on DSA); and
- RSA for Digital Signature (refer to Section 5.2.6 for introduction on RSA for Digital Signature).

5.2.9 XML Message Encryption

Standard on XML Message Encryption is required to encrypt and decrypt digital content (including XML documents and portions thereof) and to define a syntax to represent the encrypted content and information that enables an intended recipient to decrypt it.

Recommended standard / specification:

- XML Encryption Syntax and Processing.

XML Encryption Syntax and Processing	
Description	XML Encryption is a standard for encrypting/decrypting digital content (including XML documents and portions thereof) and an XML syntax used to represent the (1) encrypted content and (2) information that enables an intended recipient to decrypt it.
Reference	XML Encryption Syntax and Processing Standard is developed and recommended by W3C. The standard is available at http://www.w3.org/TR/xmlenc-core/.
Rationale for Selection	▪ XML Encryption is a W3C candidate recommendation, and is the only available standard for XML message encryption. ▪ In March 2002 the W3C XML Encryption Working Group published an XML Encryption Requirements W3C Note, and Candidate Recommendations of XML Encryption Syntax and Processing. The specifications have already satisfied the implementation requirements necessary to exit Candidate Recommendation.
Limitation	No known limitation on use of this standard.

5.2.10 XML Message Signature

Standard on XML Message Signature is required for digital signing of XML messages and its applications.

Recommended standard / specification:

- XML Signature Syntax and Processing.

XML Signature Syntax and Processing	
Description	XML Signature is a standard for digital signing of XML and its applications. The standard defines a schema for capturing the result of a digital signature operation applied to arbitrary (but often XML) data. Like non-XML-aware digital signatures (e.g., PKCS), XML signatures add authentication, data integrity, and support for non-repudiation to the data that they sign. However, unlike non-XML digital signature standards, XML signature has been designed to both account for and take advantage of the Internet and XML. A fundamental feature of XML Signature is the ability to sign only specific portions of the XML tree rather than the complete document. An XML signature can sign more than one type of resource. For example, a single XML signature might cover character-encoded data (HTML), binary-encoded data (a JPG), XML-encoded data, and a specific section of an XML file.
Reference	XML Signature Syntax and Processing standard is jointly developed and recommended by W3C and IETF. The standard is defined in RFC 3275 as well as at

XML Signature Syntax and Processing	
	http://www.w3.org/TR/xmldsig-core/ .
Rationale for Selection	▪ XML Signature is a joint W3C/IETF standard, and the only one available for XML message signing. ▪ Currently, only one version of XML Signature exists. ▪ Publicly available toolkits and software development kits are provided by market leading security vendors, including IBM, HP, Microsoft, RSA and Verisign.
Limitation	No known limitation on use of this standard.

5.2.11 Privacy Policy

Privacy policies allow users to understand the privacy practices of a site, including information concerning the data that is collected about them. Users are required to read the individual privacy policies of each site they visit in order to determine whether or not the policy is consistent with their preferences. Furthermore, sites present their policies in different ways. Privacy policy standards will define a standard format for the expression of privacy policies and automate the processes of comparing the privacy policy with user preferences and highlighting any discrepancies.

Recommended standard / specification:

- Platform for Privacy Preferences Project (P3P) version 1.0.

Platform for Privacy Preferences Project (P3P) version 1.0	
Description	P3P enables web sites to express privacy practices in a standardized form that can be automatically retrieved and interpreted by user agents, such as browsers. User agents can compare the privacy

Platform for Privacy Preferences Project (P3P) version 1.0	
	practices with the user's preferences and automatically flag differences, allowing the user to respond accordingly.
Reference	P3P v1.0 is a W3C Recommendation defined at http://www.w3.org/TR/P3P/.
Rationale for Selection	▪ P3P is a W3C recommended standard, and the only viable one available. ▪ P3P v1.0 was issued as a W3C recommendation and is thus deemed to be stable and suitable for widespread adoption. ▪ P3P is supported by the latest version of some dominant browsers such as Microsoft IE v6.0 and Mozilla (see http://www.mozilla.org/projects/p3p/). Browser plug-ins, such as AT&T's privacy bird, and policy generators such as IBM's P3P policy editor, and tools to validate P3P implementations, such as the W3C's P3P validator, are available.
Limitation	No known limitation on use of this standard.

6. RECOMMENDATIONS FOR METADATA

6.1 Overview

Metadata covers a core set of elements that contain data needed for the effective retrieval and management of official information in order to meet the Government's information management and retrieval needs.

Interoperability component covered in the Metadata area is:

- Metadata Elements and Refinements.

6.2 Recommended Standards / Specifications

6.2.1 Metadata Elements and Refinements

Standard on Metadata Elements and Refinements is required to define the elements, refinements and encoding schemas to be used by Government employees when creating metadata for their information resources or designing search systems for information systems.

Recommended standard / specification:

- Malaysian Data Dictionary Sektor Awam (DDSA).

Malaysian Data Dictionary Sektor Awam	
Description	DDSA lists the elements and refinements that will be used by the Malaysian Public Sector to create metadata for information resources. It enables users, seekers and owners of information resources to find and manage them. It also gives guidance on the purpose and use of each element.
Reference	Malaysian DDSA is developed and defined by MAMPU. This

Malaysian Data Dictionary Sektor Awam	
	standard is available at http://www.mampu.gov.my/DDSA/Intro.htm.
Rationale for Selection	▪ This is the *de facto* standard for Malaysian Government agencies and departments to specify the metadata for their information resources.
Limitation	No known limitation on use of this standard.

7. ACKNOWLEDGEMENT OF REFERENCES

Acknowledgement to the owners of the various references, standards and specifications referred and listed above.

7.1 Government Interoperability Framework Best Practices

Acknowledgement of references for best practices of Government Interoperability Framework:

- e-Government Interoperability Framework (e-GIF) Version 4.0 (published on 25th April 2002) and Version 5.0 (published on 25th April 2003),
  - Office of the e-Envoy, Cabinet Office, United Kingdom;
- The HKSARG Interoperability Framework Version 1.0 (published in November 2002)
  - Information Technology Services Department, The Government of the Hong Kong Special Administrative Region (HKSARG).

7.2 International Standard Organisations

Acknowledgement of major references for international technical standards and specifications:

- Internet Engineering Task Force (IETF)
  - http://www.ietf.org;
- International Standards Organisation (ISO)
  - http://www.iso.org; and
- World Wide Web Consortium (W3C)
  - http://www.w3c.org.

Acknowledgement of other references for international technical standards and specifications:

- American National Standards Institute (ANSI)
  - http://www.ansi.org;
- ECMA International
  - http://www.ecma-international.org;
- Institute of Electrical and Electronics Engineers (IEEE)
  - http://www.ieee.org;
- National Institute of Standards and Technology (NIST)
  - http://www.nist.gov;
- Object Management Group (OMG)
  - http://www.omg.org;
- Open Mobile Alliance (OMA) and WAP Forum
  - http://www.openmobilealliance.org and http://www.wapforum.org;
- Organization for the Advancement of Structured Information Standards (OASIS)
  - http://www.oasis-open.org; and
- Unicode, Inc.
  - http://www.unicode.org.

7.3 IT Industry Organisations

Acknowledgement of references for technical standards and/or product specifications:

- Adobe Systems Incorporated
  - http://www.adobe.com;
- Apple Computer, Inc.
  - http://www.apple.com;
- Macromedia, Inc.
  - http://www.macromedia.com;
- Microsoft Corporation
  - http://www.microsoft.com;

- Netscape Communications Corporation
  - http://www.netscape.com;
- PKWARE, Inc.
  - http://www.pkware.com;
- Real Networks, Inc.
  - http://www.realnetworks.com; and
- RSA Laboratories
  - http://www.rsasecurity.com.

8. ABBREVIATIONS AND ACRONYMS

The list of abbreviations and acronyms used in MyGIF is listed below for easy reference.

Abbreviations and Acronyms used in MyGIF

3DES	Triple Data Encryption Standard
3G	Third Generation Mobile Phones
AH	Authentication Header
ANS	American National Standards
ANSI	American National Standards Institute (USA)
ASCII	American Standard Code for Information Interchange
BEA	BEA Systems, Inc.
CCS	Coded Character Set
CDMA	Code Division Multiple Access
CSV	Comma Separated Variable
DDSA	Data Dictionary Sektor Awam
DES	Data Encryption Standard
DNS	Domain Name System
DNS RR	DNS Resource Record
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECMA	European Computer Manufacturers Association
e-GIF	e-Government Interoperability Framework (UK)
EGIT	Electronic Government Information Technology Policy and Standards
e-GMS	e-Government Metadata Standard (UK)
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GIF	Graphic Interchange Format
GNU	GNU's Not Unix'
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GZIP	GNU Zip
HKSARG	The Government of Hong Kong Special Administrative Region
HP	Hewlett-Packard

Abbreviations and Acronyms used in MyGIF

HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines Corporation
IE	Internet Explorer (Microsoft)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISO	International Organisation for Standardization
IT	Information Technology
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAMPU	Malaysian Administrative Modernisation & Management Planning Unit
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MyMIS	Malaysian Public ICT Management Security Handbook
NIST	National Institute of Standards and Technology (USA)
NNTP	Network News Transfer Protocol
NSA	National Security Agency (USA)
NTT	NTT Mobile Communications Network, Inc.
OASIS	Organization for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
OMG	Object Management Group
P3P	Platform for Privacy Preferences Project
PDA	Personal Digital Assistant
PDF	Portable Document Format
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
POP	Post Office Protocol
FIPS PUB	FIPS Publication

Abbreviations and Acronyms used in MyGIF

QoS	Quality of Service
RDF	Resource Description Framework
RFC	Request for Comments
RPCs	Remote Procedure Calls
RSA	Rivest-Shamir-Adleman
RTF	Rich Text Format
S/MIME	Secure Multipurpose Internet Mail Extensions
SAP	SAP AG
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transport Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDMA	Time-Division Multiple Access
TIFF	Tag Image File Format
TLS	Transport Layer Security
UCS	Universal Multiple-Octet Coded Character Set
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UK	United Kingdom
UML	Unified Modelling Language
US	United States of America
UTF	UCS Transformation Format
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WAP	Wireless Application Protocol
WML	Wireless Markup Language
WMP	Windows Media Player
WSDL	Web Services Description Language
WWW	World Wide Web
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language

Abbreviations and Acronyms used in MyGIF

XPath	XML Path Language
XSL	XML Stylesheet Language
XSLT	XSL Translation