

**Office of the
Government Chief Information Officer**

**Analysis Underpinning
The HKSARG Interoperability Framework
Recommendations**

Version: 7.0 Draft

October 2008

The Government of the Hong Kong Special Administrative Region

COPYRIGHT NOTICE

© 2008 by the Government of the Hong Kong Special Administrative Region

Unless otherwise indicated, the copyright in the works contained in this publication is owned by the Government of the Hong Kong Special Administrative Region. You may generally copy and distribute these materials in any format or medium provided the following conditions are met –

- (a) the particular item has not been specifically indicated to be excluded and is therefore not to be copied or distributed;
- (b) the copying is not done for the purpose of creating copies for sale;
- (c) the materials must be reproduced accurately and must not be used in a misleading context; and
- (d) the copies shall be accompanied by the words “copied/distributed with the permission of the Government of the Hong Kong Special Administrative Region. All rights reserved.”

If you wish to make copies for purposes other than that permitted above, you should seek permission by contacting the Office of the Government Chief Information Officer.

Distribution of Controlled Copy	
Copy No.	Holder
1	Government-wide Intranet (itginfo.ccgo.hksarg)
2	Internet (www.ogcio.gov.hk)

Prepared By: Interoperability Framework Coordination Group

Doc. Effective Date: 1 March 2009

Amendment History				
Change Number	Revision Description	Sections Affected	Revision Number	Date
	Major updates to version 6.0 issued in December 2007 are as follows :		7.0 Draft	MMM 2008
1.	Update the description of UDDI v2.	3.1.2.1		
2.	Update the description of CORBA.	3.1.2.1		
3.	Update the forward outlook of ebMS v2.	3.1.2.2		
4.	Update the standards for future consideration.	3.1.4.1		
5.	Add a new interoperability area “Portable virtual machine package” for future consideration with OVF as an emerging standard.	3.1.4.2		
6.	Add a new interoperability area “IT service modeling” for future consideration with SML as an emerging standard.	3.1.4.3		
7.	Update the maturity of PDF.	3.2.1.4		
8.	Rename the recommended specification “PDF 1.7” to “PDF 1.7 (ISO 32000-1)”.	3.2.1.5 3.2.1.6		
9.	Replace “Microsoft Internet Explorer v6.x and Mozilla Firefox v1.5.x” by “Microsoft Internet Explorer 6/7 and Mozilla Firefox 2.0.x/3.0.x” in the remarks of “Document file type for receiving documents under ETO” interoperability area.	3.2.1.5		
10.	Remove specification “.sxw” from the “Formatted document file type for collaborative editing” interoperability area.	3.2.1.7		
11.	Remove specification “.sxi” from the “Presentation file type for collaborative editing” interoperability area.	3.2.1.8		

Amendment History				
Change Number	Revision Description	Sections Affected	Revision Number	Date
12.	Remove specification “.sxc” from the “Spreadsheet file type for collaborative editing” interoperability area.	3.2.1.9		
13.	Revise the emerging specifications “Office Open XML (.docx)”, “Office Open XML (.xlsx)” and “Office Open XML (.pptx)” to “ISO/IEC DIS 29500 (Office Open XML)”.	3.2.1.7 3.2.1.8 3.2.1.9		
14.	Update the description of ISO/IEC DIS 29500 (Office Open XML).	3.2.1.7		
15.	Update the remarks of “Character sets and encoding for Web content” interoperability area.	3.2.1.13		
16.	Update the forward outlook of ISO/IEC 8859-1:1998.	3.2.1.13		
17.	Update the forward outlook and limitations on the use of BIG-5.	3.2.1.13		
18.	Update the maturity, version and rationale of ISO/IEC 10646-1:2000.	3.2.1.13		
19.	Update the forward outlook of HKSCS-2001.	3.2.1.13		
20.	Update the remarks of “Character sets and encoding for other types of information exchange” interoperability area.	3.2.1.14		
21.	Update the description of XForms.	3.2.3.2		
22.	Update the description of WS-Federation.	3.3.1.16		
23.	Add “IEEE 802.11n” as a specification under observation in the area “Wireless LAN”.	3.4.1.9		
24.	Add WPA2 as a recommended specification in the area “Wireless LAN security”.	3.4.1.10		

TABLE OF CONTENTS

1.	INTRODUCTION	1-1
2.	ORGANISATION OF THE TECHNICAL STANDARDS.....	2-1
3.	ANALYSIS OF TECHNICAL STANDARDS UNDER THE IF	3-1
3.1	APPLICATION INTEGRATION DOMAIN	3-1
3.1.1	Overview	3-1
3.1.2	Interoperability areas for immediate consideration	3-3
3.1.2.1	<i>Simple functional integration in an open environment</i>	<i>3-3</i>
3.1.2.2	<i>Reliable message exchange between application systems in an open environment for business document-oriented collaboration.....</i>	<i>3-7</i>
3.1.2.3	<i>Secure exchange of messages in a Web Services environment</i>	<i>3-9</i>
3.1.3	Interoperability areas for future consideration – no apparent need yet	3-10
3.1.3.1	<i>Information model for e-business registry</i>	<i>3-10</i>
3.1.3.2	<i>E-business registry service.....</i>	<i>3-11</i>
3.1.3.3	<i>Transport-neutral mechanisms to address Web Services and messages</i>	<i>3-11</i>
3.1.3.4	<i>Grammar for expressing the capabilities, requirements, and general characteristics of entities in an XML Web Services-based system.....</i>	<i>3-12</i>
3.1.4	Interoperability areas for future consideration – standards not matured yet	3-12
3.1.4.1	<i>Intra-government workflow and business process management.....</i>	<i>3-13</i>
3.1.4.2	<i>Portable virtual machine package.....</i>	<i>3-15</i>
3.1.4.3	<i>IT service modeling</i>	<i>3-16</i>
3.2	INFORMATION ACCESS AND INTERCHANGE DOMAIN.....	3-17
3.2.1	Interoperability areas for immediate consideration	3-17
3.2.1.1	<i>Hypertext Web content</i>	<i>3-17</i>
3.2.1.2	<i>Client-side scripting</i>	<i>3-19</i>
3.2.1.3	<i>Mobile Web content.....</i>	<i>3-20</i>
3.2.1.4	<i>Document file type for content publishing</i>	<i>3-22</i>
3.2.1.5	<i>Document file type for receiving documents under ETO</i>	<i>3-23</i>
3.2.1.6	<i>Attachment of digital signature to electronic documents received under ETO</i>	<i>3-25</i>
3.2.1.7	<i>Formatted document file type for collaborative editing.....</i>	<i>3-27</i>
3.2.1.8	<i>Presentation file type for collaborative editing.....</i>	<i>3-30</i>
3.2.1.9	<i>Spreadsheet file type for collaborative editing.....</i>	<i>3-32</i>
3.2.1.10	<i>E-mail format.....</i>	<i>3-33</i>
3.2.1.11	<i>E-mail security.....</i>	<i>3-34</i>
3.2.1.12	<i>Graphical / Image File Types.....</i>	<i>3-36</i>
3.2.1.13	<i>Character sets and encoding for Web content</i>	<i>3-38</i>
3.2.1.14	<i>Character sets and encoding for other types of information exchange</i>	<i>3-41</i>
3.2.1.15	<i>Compressed files.....</i>	<i>3-43</i>
3.2.1.16	<i>Removable storage media for receiving documents under the ETO</i>	<i>3-44</i>
3.2.1.17	<i>Animation</i>	<i>3-46</i>
3.2.1.18	<i>Moving image and audio/visual</i>	<i>3-47</i>
3.2.1.19	<i>Audio/video streaming.....</i>	<i>3-50</i>
3.2.1.20	<i>E-business document / data message formatting language.....</i>	<i>3-51</i>
3.2.1.21	<i>XML schema definition.....</i>	<i>3-52</i>
3.2.1.22	<i>XML message encryption</i>	<i>3-54</i>

3.2.1.23	<i>XML message signing</i>	3-55
3.2.1.24	<i>Content syndication</i>	3-56
3.2.2	Interoperability areas for future consideration – no apparent need yet	3-57
3.2.2.1	<i>Vector graphics (non GIS/mapping application)</i>	3-57
3.2.2.2	<i>Content/data resource description language</i>	3-58
3.2.3	Interoperability areas for future consideration –standards not matured yet	3-59
3.2.3.1	<i>Inter-organisation radio frequency identification</i>	3-59
3.2.3.2	<i>Electronic form</i>	3-61
3.3	SECURITY DOMAIN	3-61
3.3.1	Interoperability areas for immediate consideration	3-61
3.3.1.1	<i>IP network-level security</i>	3-61
3.3.1.2	<i>Transport-level security</i>	3-63
3.3.1.3	<i>Symmetric encryption algorithms</i>	3-65
3.3.1.4	<i>Asymmetric encryption algorithms</i>	3-67
3.3.1.5	<i>Digital signature algorithms</i>	3-69
3.3.1.6	<i>Hashing algorithms for digital signature</i>	3-71
3.3.1.7	<i>Cryptographic message syntax for file-based signing and encrypting</i>	3-72
3.3.1.8	<i>On-line certificate status protocol</i>	3-73
3.3.1.9	<i>Certification request</i>	3-74
3.3.1.10	<i>Certificate profile</i>	3-75
3.3.1.11	<i>Certificate revocation list profile</i>	3-76
3.3.1.12	<i>Certificate import/export interface</i>	3-77
3.3.1.13	<i>Cryptographic token interface</i>	3-78
3.3.1.14	<i>Cryptographic token information syntax</i>	3-80
3.3.1.15	<i>Privacy policy</i>	3-81
3.3.1.16	<i>Exchange of authentication and authorisation Information</i>	3-82
3.3.1.17	<i>Time stamping protocol</i>	3-84
3.3.2	Interoperability areas for future consideration – standards not matured yet	3-85
3.3.2.1	<i>XML-based authorisation and entitlement</i>	3-85
3.3.2.2	<i>XML key management</i>	3-86
3.4	INTERCONNECTION DOMAIN	3-86
3.4.1	Interoperability areas for immediate consideration	3-86
3.4.1.1	<i>E-mail transport</i>	3-86
3.4.1.2	<i>Mail box access</i>	3-87
3.4.1.3	<i>Hypertext transfer protocol</i>	3-89
3.4.1.4	<i>Directory access</i>	3-90
3.4.1.5	<i>Domain name service</i>	3-91
3.4.1.6	<i>File transfer</i>	3-92
3.4.1.7	<i>LAN/WAN interworking</i>	3-94
3.4.1.8	<i>LAN / WAN transport protocol</i>	3-96
3.4.1.9	<i>Wireless LAN</i>	3-97
3.4.1.10	<i>Wireless LAN security</i>	3-99
3.4.1.11	<i>Mobile device Internet access</i>	3-101

1. INTRODUCTION

This report documents the detailed information resulting from the research and analysis conducted in the development of the Interoperability Framework (IF). It contains the background data from which the recommended standards published in the HKSARG Interoperability Framework¹ have been derived.

This report is intended for reference by bureaux and departments (B/Ds) and their contractors.

Feedback on this report from B/Ds and their contractors is welcomed, and comments should be sent to the Interoperability Framework Co-ordination Group (IFCG) (ifcg@ogcio.gov.hk).

¹ Internet: <http://www.ogcio.gov.hk/eng/infra/eif.htm>
Intranet: <http://itginfo.cgo.hksarg/content/if/index.htm>

2. ORGANISATION OF THE TECHNICAL STANDARDS

From a joined-up service project's perspective, the interoperability specifications that the collaborating parties have to agree upon can be classified into 5 domains:

- Business specific – business-oriented specifications such as business function interaction models, message content and semantics for data interchange between applications, etc.;
- Application integration – technical specifications to enable application-to-application integration;
- Information access and interchange – technical specifications for file exchange, character sets and encoding, etc.;
- Security – technical specifications to enable the secure exchange of information;
- Interconnection – technical specifications to enable communication between systems.

With regard to the business specific domain, the collaborating parties have to agree on the business-oriented specifications based upon their business requirements. With regard to the other 4 domains, the collaborating parties should adopt the technical standards recommended under the IF, where relevant.

Section 3 provides an analysis of these technical standards. Under each of these 4 domains, interoperability areas have been identified. Most of these interoperability areas are for immediate consideration while a few have been classified for future consideration either because the standards are immature or because the business needs are not apparent in the HKSARG yet.

Section 3 describes, under each domain, the areas included for immediate consideration and for future consideration.

Under each area, the relevant technical standards are described. Apart from recommending the standards for immediate adoption, we also recommend emerging standards for close monitoring and potential future adoption.

In some cases, multiple specifications are recommended for an interoperability area. In these cases, where necessary, the IF will provide remarks to help project teams choose among the recommended standards, or for addressing interoperability issues in an environment where multiple standards are used.

The IF also indicates for each area whether the standards for that area are intended to be relevant for electronic submissions under the Electronic Transactions Ordinance (ETO). Some of these standards may not be reflected in the prevailing Format and Manner Requirements published by the Permanent Secretary for Commerce and Economic Development (Communications and Technology) pursuant to the ETO, however, they are intended to be promulgated in future government notices to be published in relation to the Format and Manner Requirements.

Each selected standard is described and justified along with supporting information. This information contains the following:

- Short description
- Rationale for selection
- Maturity
- Forward outlook
- Version, where appropriate, and rationale
- Any usage limitations

3. ANALYSIS OF TECHNICAL STANDARDS UNDER THE IF

3.1 APPLICATION INTEGRATION DOMAIN

3.1.1 Overview

The application integration domain comprises technical specifications to enable applications to interact in an open environment. In an open environment, such interactions are intrinsically message based; and the messages can either be document-oriented or procedure-oriented (Remote Procedure Call type).

As the purpose of the interaction is to realize business collaboration involving multiple parties (i.e. to perform a joined-up service), it can be viewed as a sort of workflow, involving a sequence of message (including acknowledgement) exchanges among the stakeholders. The collection of messages exchanged for a particular “business transaction” is often called a conversation.

To automate such a workflow, individual applications need to address many interaction aspects, e.g.

- The reliable delivery of messages from one application to another, or be informed of the delivery error when the message cannot be delivered;
- Security aspects such as message integrity and confidentiality, or a message-receiving application’s need to authenticate the message sending application or to check the authority of a person trying to trigger some business function;
- The correlation of messages associated with a conversation;
- The ability to concertedly abort a business transaction across all interacting applications if deemed appropriate;
- The ability to respond accordingly (and take other relevant actions) based on the business rules defined in the interaction contract or an organisation’s internal policy; etc.

Standard ways to address these aspects are beginning to emerge, but few of these standards are matured yet. Therefore, comprehensive integration of collaborating applications currently requires the interacting parties to agree on the application integration specifications on a case-by-case basis.

Currently there are two major streams of application integration standards, namely:

- ebXML; and
- Web Services based around a core set of standards : SOAP, WSDL and UDDI.

ebXML is an initiative which aims to achieve comprehensive integration. It started as an initiative sponsored by UN/CEFACT and OASIS. However, on 21 August 2003, UN/CEFACT announced the completion of the ebXML technical standards work programme with OASIS. That announcement also mentioned that while UN/CEFACT will remain open to working with OASIS in the future, the

UN/CEFACT Plenary meeting has directed a new work programme to move UN/CEFACT closer to Web Services and this new work programme is called the UN/CEFACT Business Collaboration Framework (BCF).

ebXML aims to enable organisations of all sizes to conduct electronic business over the Internet. A second goal of ebXML is to provide an alternative to the use of EDI value added networks (VANS). With UN/CEFACT's experience in EDI, ebXML has set out to solve a well-defined problem: the automation of the interaction between businesses. ebXML first defines the requirements for conducting e-business and then defines specifications to meet those requirements. The result is a well-architected suite of specifications, comprising technical standards and generic / industry-specific standard business processes.

The ebXML suite includes specifications for :

- Reliable messaging (ebXML Message Service Specification)
- Describing capabilities in terms of the type of messaging, process specifications, document schemas which describe public interfaces (Collaboration Protocol Profiles)
- Describing agreements in terms of technical capabilities and business requirements, such as response times, problem management (Collaboration Protocol Agreements)
- Describing document exchange processes and business process definitions (Business Process Specification Schema)
- Registry repository to store and locate business documents, business process definitions, Collaboration Protocol Profiles and Collaboration Protocol Agreements (Registry Information Model and Registry Services)
- Defining common components to address differences in terminology and documents between different vertical industries (Core Component Technical Specification).

Individual ebXML specifications can be separately and progressively applied to meet business requirements. They do not necessarily have to be applied at the same time.

At the same time, the industry is promoting Web Services, based around a core set of standards: SOAP, WSDL and UDDI. The initial focus of Web Services is to enable functional integration based on implementation-independent specifications for describing, executing and locating remote services. Additional specifications are being defined to address higher-level functionality, such as reliable messaging, security, transaction management, business process management, orchestration, etc.

The standards under the ebXML suite and those under the Web Services suite may not be compatible. Adaption (or customization) may be necessary if a project needs to mix the use of standards from these 2 suites.

Currently, the standards for application integration are not sufficiently mature to address all potential requirements. Given these constraints, the IF defines only those specifications which are matured for adoption. This limited set of specifications will allow project teams to implement simple business collaboration where the shortcomings of the current specifications are not significant (e.g. simple read-only request-response transactions) or where the shortcomings can be addressed in ways which do not impact interoperability (e.g. transaction management is integral to one of the participating applications).

3.1.2 Interoperability areas for immediate consideration

3.1.2.1 Simple functional integration in an open environment

Justification for inclusion and usage

The standards in this area allow an application to expose its functionality through an open interface for remote access by other applications running on heterogeneous platforms. Currently, the industry has generally agreed on the adoption of a set of core standards for such procedure-oriented integration. However, these standards by themselves can only enable simple functional integration (**such as information retrieval from a remote application**). Additional handshake protocols need to be agreed among the interacting parties to enable more complex integration, such as those involving transaction integrity.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
The suite of core Web Services standards CORBA DCOM RMI WSIL	The suite of core Web Services standards: SOAP v1.1 for remote service invocation WSDL v1.1 for remote service description (where necessary) UDDI v2 for the publication and discovery of remote service descriptions	WSIL for locating WSDLs directly from the service provider's site
Remarks: When project teams select products to implement Web Services, they are recommended to take into consideration the products' conformance to the WS-I's Basic Profile 1.1. In addition, project teams should implement their Web Services requests and responses in accordance with the WS-I Basic Profile 1.1.		

Recommended standards

Standard 1a Simple Object Access Protocol (SOAP) v1.1	
Description	Simple Object Access Protocol (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

Standard 1a Simple Object Access Protocol (SOAP) v1.1	
	<p>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.</p>
Rationale for selection	<p>SOAP is being developed by the W3C XML Protocol Working Group as part of the Web Services Activity.</p> <p>SOAP is one of the core technologies which underpins Web Services and has significant industry support from a broad range of infrastructure and application providers.</p> <p>SOAP is included in the WS-I (Web Services Interoperability) Basic Profile.</p> <p>In contrast to CORBA, DCOM and RMI, the use of SOAP is independent of the way that the applications to be integrated are developed.</p>
Maturity	<p>SOAP v1.1 was published as a W3C Note in May 2000.</p>
Forward outlook	<p>On 24 June 2003, W3C released SOAP Version 1.2 as a W3C Recommendation.</p>
Version and rationale for version	<p>SOAP v1.1 remains as the recommended standard because SOAP v1.2 does not form part of the WS-I Basic Profile yet.</p>
Limitations on the use of this standard	<p>Interoperability between different implementations of the Web Services specifications cannot be guaranteed yet. As such, it is strongly recommended that B/Ds take this into account during implementation and consider limiting initial deployments to a restricted number of integrations (i.e., before Web Services interoperability is mature, deploy Web Services specifications between pre-defined systems under a well-tested environment, rather than deploying them for openly accessible services). Limiting the number and range of interactions will assist in managing any incompatibility issues which arise.</p> <p>It is recommended that progress of the Web Services Interoperability Organisation (WS-I) is closely monitored (see http://www.ws-i.org). WS-I is an industry body with a charter to “promote Web Services interoperability across platforms, operating systems, and programming languages. The organisation works across the industry and standards organisations to respond to customer needs by providing guidance, best practices, and resources for developing Web Services solutions.”</p>

Standard 1b Web Services Description Language (WSDL) v1.1	
Description	<p>Web Services Description Language (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.</p>
Rationale for selection	<p>WSDL is the basis of the work of the Web Services Description Working Group of the W3C’s Web Services Activity.</p> <p>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.</p> <p>WSDL is included in the WS-I Basic Profile.</p>
Maturity	<p>Version 1.1 (the basis of the W3C Web Services Description Working Group) was submitted to the W3C as a suggestion for describing services in March 2001.</p>

Standard 1b Web Services Description Language (WSDL) v1.1	
Forward outlook	WSDL v2.0 became a W3C Recommendation in June 2007.
Version and rationale for version	Version 1.1, which is part of the WS-I Basic Profile.
Limitations on the use of this standard	<p>Interoperability between different implementations of the Web Services specifications cannot be guaranteed yet. As such, it is strongly recommended that B/Ds take this into account during implementation and consider limiting initial deployments to a restricted number of integrations (i.e., before Web Services interoperability is mature, deploy Web Services specifications between pre-defined systems under a well-tested environment, rather than deploying them for openly accessible services). Limiting the number and range of interactions will assist in managing any incompatibility issues which arise.</p> <p>It is recommended that progress of the Web Services Interoperability Organisation (WS-I) is closely monitored (see http://www.ws-i.org). WS-I is an industry body with a charter to “promote Web Services interoperability across platforms, operating systems, and programming languages. The organisation works across the industry and standards organisations to respond to customer needs by providing guidance, best practices, and resources for developing Web Services solutions.”</p>

Standard 1c Universal Description, Discovery and Integration (UDDI) v2	
Description	<p>Universal Description, Discovery and Integration (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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>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.</p> <p>It should be noted that the registration of Web service instances in UDDI registries is optional. By no means do all usage scenarios require the kind of metadata and discovery UDDI provides, but where such capability is needed, UDDI is the sanctioned mechanism for Web Services.</p>
Rationale for selection	<p>UDDI is an industry initiative, involving more than 220 IT and user companies. It is the intention of UDDI.org to submit the specification to a standards body after the completion of version 3 of the specification.</p> <p>As indicated by WS-I, UDDI is the sanctioned mechanism for the publication and discovery of Web Services when such function is needed.</p> <p>UDDI has broad industry recognition as a solution to enable the publication and location of services described using WSDL and requested using SOAP.</p>

Standard 1c Universal Description, Discovery and Integration (UDDI) v2	
Maturity	Version 1 of the UDDI specification was published in September 2000. Version 2 was published in June 2001 and was approved as an OASIS Open Standard on 20 May 2003. Version 2 of the specification is being adopted by common public repositories and product vendors.
Forward outlook	UDDI v3 became an OASIS Standard in February 2005.
Version and rationale for version	Version 2, which has wide product support.
Limitations on the use of this standard	The Web Services that constitute UDDI v2 are not fully conformant with the WS-I Basic Profile 1.0 because they do not accept messages encoded in both UTF-8 and UTF-16 as required by the Profile. (They accept UTF-8 only.) That there should be such a discrepancy is hardly surprising given that UDDI V2 was designed and, in many cases, implemented before the Profile was developed. UDDI's designers are aware of UDDI V2's non-conformance and will take it into consideration in their future work.

Emerging standards for future consideration

Emerging Standard(s)	Description
WSIL – for locating WSDLs directly from the service provider's site	<p>Web Services Inspection Language (WSIL) is a joint initiative between Microsoft and IBM, designed to allow service providers to provide references to service descriptions directly, rather than in a centralised repository such as a UDDI Business Registry. WSIL is thus not designed to enable discovery where the provider is not known and is thus suited only to existing relationships.</p> <p>WSIL defines:</p> <ul style="list-style-type: none"> • an XML format for listing references to service descriptions; • a set of conventions to make it easy to locate WS-Inspection documents i.e. how to inspect a web site for available Web Services and the locations on a web site where those web service descriptions may be found. <p>Service descriptions can be defined in multiple formats, including WSDL and HTML. It is possible for the same service to be described in multiple formats.</p> <p>WSIL was proposed by IBM and Microsoft in November 2001 but is yet to be submitted to a standards body. The evolution of WSIL should be closely monitored for consideration as a standard for Publication of Remote Services.</p>

Other Candidate Standards

Other Standard(s)	Description
Common Object Request Broker Architecture (CORBA)	<p>CORBA is an architecture and specification developed through the Object Management Group, sanctioned by ISO, as a standard for distributed objects. The current version of CORBA is 3.1. CORBA uses the Internet Inter-ORB Protocol (IIOP) for remote request delivery and Interface Definition Language (IDL) for remote service description.</p> <p>IIOP and IDL are not recommended as standards for generic application-to-application integration because their use presupposes an application development architecture, as well as an integration architecture, based on CORBA. SOAP and WSDL in contrast, provide an integration mechanism which is independent of the architecture used for application development. It is possible to wrap legacy CORBA-based applications using WSDL to enable integration of such applications.</p>

Other Standard(s)	Description
Distributed Component Object Model (DCOM)	<p>DCOM is a set of Microsoft concepts and program interfaces in which client program objects can request services from server program objects on other computers in a network. DCOM is based on the Component Object Model (COM), which provides a set of interfaces allowing clients and servers to communicate within the same computer.</p> <p>DCOM is not recommended as a standard for generic application-to-application integration as it is implementation-specific and presupposes that application development and integration is based on DCOM which is specific to Microsoft platforms. SOAP and WSDL, in contrast, provide an integration mechanism which is independent of the architecture used for application development. It is possible to wrap existing DCOM-based applications using WSDL to enable integration of such applications.</p>
Remote Method Invocation (RMI)	<p>RMI is part of the Java 2 Enterprise Edition (J2EE) specification. RMI is a form of remote procedure call (RPC), based on the use of client proxies, a remote reference layer for marshalling requests and a transport connection layer which sets up and manages the request.</p> <p>RMI is not recommended as a standard for generic application-to-application integration as it presupposes the use of J2EE for application development and is thus implementation-specific. SOAP and WSDL, in contrast, provide an integration mechanism which is independent of the architecture used for application development. It is possible to wrap existing J2EE-based applications using WSDL to enable integration of such applications.</p>

3.1.2.2 Reliable message exchange between application systems in an open environment for business document-oriented collaboration

Justification for inclusion and usage

Defines the protocol for the guaranteed delivery of documents between application systems in document-oriented B2G or G2G collaboration.

Relevant to submissions under ETO : B/Ds will promulgate explicit requirements where relevant

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
ebMS WS-Reliability WS-ReliableMessaging WS-Transaction ebXML CPPA	ebMS v2 (ISO/TS 15000-2:2004)	WS-Reliability WS-ReliableMessaging ebXML CPPA WS-Transaction
<p>Remarks: Standards for reliable messaging are also emerging under the Web Services framework. Joined-up applications that are following Web Services standards should agree among the stakeholders on whether to adopt ebMS or some alternate protocol for reliable message exchange.</p>		

Recommended standards

Standard 1 ebXML Message Service (ebMS) v2 (ISO/TS 15000-2:2004)	
Description	<p>The ebXML Message Service Specification is one of the specifications within the ebXML framework of specifications.</p> <p>This specification defines the ebXML Message Service Protocol which enables the secure and reliable exchange of messages between two parties. It includes descriptions of the message structure used to package payload data for transport and the behaviour of the message service handler responsible for sending and receiving messages.</p> <p>This specification is independent of both the payload and the communications protocol used.</p> <p>It utilises W3C's XML Signature standard to provide secure SOAP messaging.</p> <p>ebMS defines an interoperable protocol where any two Message Service implementations can reliably exchange messages sent using once-and-only-once delivery semantics.</p>
Rationale for selection	<p>Among the similar initiatives for reliable messaging (such as WS-ReliableMessaging and WS-Reliability), ebMS is the most mature one and has quite a number of successful implementations in the ebXML community.</p>
Maturity	<p>The OASIS ebXML Implementation, Interoperability and Conformance (IIC) Technical Committee (TC) has approved ebMS v2 in May 2003. ebMS was also published as ISO standard (ISO/TS 15000-2:2004) in 2004.</p>
Forward outlook	<p>OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features became an OASIS Standard in October 2007. It supports networking topologies with only a point-to-point (Messaging Service Handler) MSH topology, in which no intermediaries are present.</p> <p>A forthcoming Part 2, containing Advanced Features, may take into account topologies that contain intermediaries (e.g. hub, multi-hop), as well as those in which the ultimate MSH acts as a SOAP intermediary.</p>
Version and rationale for version	<p>Version 2.0, which has been approved by OASIS ebXML Implementation, Interoperability and Conformance (IIC) Technical Committee (TC).</p>
Limitations on the use of this standard	<p>ebMS is not designed to be part of the Web Services framework, although ebMS also uses a SOAP envelop. Projects using Web Services standards should agree among the stakeholders on whether to adapt ebMS or to adopt some alternate protocol for reliable message exchange.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
WS-Reliability	<p>WS-Reliability specification 1.0 was submitted to OASIS Web Services Reliable Messaging TC by Fujitsu, Hitachi, NEC, Oracle, Sonic Software & Sun in early 2003. WS-Reliability enables reliable messaging in Web Services. WS-Reliability v1.1 was officially declared an OASIS Standard in November 2004.</p>
WS-ReliableMessaging	<p>BEA, IBM, Microsoft and TIBCO also announced their secure and reliable messaging protocol : WS-ReliableMessaging in March 2003. In May 2005, OASIS accepted the submission of WS-ReliableMessaging and formed a Web Services Reliable Exchange (WS-RX) Technical Committee (TC) for reconciliation with WS-Reliability. It became an OASIS standard in June 2007.</p>
ebXML CPPA	<p>ebXML Collaboration Protocol Profile and Agreement is one of the possible ways for specifying and agreeing upon ebMS parameters. CPPA v2.0 is an approved OASIS standard.</p>

Emerging Standard(s)	Description
WS-Transaction	WS-Transaction defines a set of protocols to coordinate the outcomes of distributed application actions. Web Services Coordination (WS-Coordination) v1.1, Web Services Atomic Transaction (WS-AtomicTransaction) v1.1 and Web Services Business Activity (WS-BusinessActivity) v1.1 were approved as OASIS standards in April 2007.

Other Candidate Standards

Other Standard(s)	Description
None	

3.1.2.3 Secure exchange of messages in a Web Services environment

Justification for inclusion and usage

To enable the exchange of signed and encrypted messages in a Web Services environment.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
WS-Security	WS-Security 1.0	WS-Security 1.1
<p>Remarks:</p> <p>Project teams should closely monitor the development of the WS-I Basic Security Profile and follow its recommendations when it is ratified.</p>		

Recommended standards

Standard 1 WS-Security 1.0	
Description	Standards such as XML Encryption and XML Signature are generic, being applicable to any XML document. Web Service security standards are necessary to enable message integrity, message confidentiality and message authentication for XML documents used in Web Services. These standards define how security is applied to SOAP messages e.g. allowing a SOAP message to be encrypted using XML Encryption and signed using XML Signature.
Rationale for selection	WS-Security v1.0 is an OASIS standard, and is an industry-wide recognized XML-based standard for securing Web Services message exchanges.
Maturity	<p>Web Services Security (WS-Security) version 1.0 has become an OASIS Standard in April 2004.</p> <p>It is supported by major platform development providers, e.g. Microsoft's Web Services Enhancement, IBM's WebSphere SDK for Web Services v5.1, and Sun's Java Web Services Developer Pack v1.4.</p> <p>It is also supported in security products such as Verisign's Trust Gateway, RSA's BSAFE Secure-WS and DataPower's XML Security Gateway.</p>

Standard 1 WS-Security 1.0	
Forward outlook	<p>OASIS WS-Security TC members envision that the approved deliverables of Web Services Security will form the necessary technical foundation for higher-level security services which are to be defined in other specifications.</p> <p>Gartner Group recommends that enterprises should adopt WS-Security formatting for all across-the-firewall Web Services deployments, even in cases where no security needs have been identified. Gartner also believes that WS-Security will be the standard for the majority of Web Services, and committing to it now will allow enterprises to easily modify the security profile of deployed Web Services in the future.</p>
Version and rationale for version	Currently, only one version of WS-Security exists.
Limitations on the use of this standard	<p>Based on experience with similar specifications, interoperability issues can easily arise in some areas. Care should be taken when implementing to avoid those issues, e.g. those related to understanding algorithm associated with Key Identifiers, as well as wrong interpretation of the SOAP, WSDL and HTTP semantics.</p> <p>The progress of the WS-I's Basic Security Profile (WS-I – http://www.ws-i.org) which focuses on delineating guidelines for key aspects of WS-Security should be closely monitored.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
WS-Security 1.1	<p>In Feb 2006, WS-Security 1.1 was proposed by OASIS for acceptance as standard. It is a revision of the original WS-Security 2004 OASIS standard. It has factored in 1.0 Errata and added several token profiles. The 1.1 schema does not replace the 1.0 schema, rather it builds upon it by defining an additional set of capabilities within a 1.1 namespace. WS-Security 1.1 includes the following new features:</p> <ul style="list-style-type: none"> ▪ Encrypted SOAP Header ▪ Token Reference to Encrypted Key ▪ Signature Confirmation ▪ Password-based Key Derivation ▪ Thumbprint References <p>Product implementation of WS-Security 1.1 specific features are still emerging in the market. Respective interoperability tests are yet to be available in the public domain.</p>

Other Candidate Standards

Other Standard(s)	Description
None	

3.1.3 Interoperability areas for future consideration – no apparent need yet

3.1.3.1 Information model for e-business registry

Justification for inclusion and usage

Defines the information model for a registry to support e-business, including the information to be stored in a registry and its organisation and structure.

Standards for future consideration

Standard(s)	Description
ebXML Registry Information Model	<p>The ebXML Registry Information Model (RIM) is one of the specifications within the ebXML framework of specifications. It defines the format and structure of a registry required to support the implementation of ebXML. Together with the ebXML Registry Services Specification, they can be used to implement an ebXML registry & repository for sharing information for business process integration.</p> <p>ebXML RIM v3.0 is the latest OASIS approved standard.</p> <p>While the ebXML RIM forms part of the ISO 15000 standard, OASIS technical committees retain the responsibility for maintaining and advancing ebXML standards.</p>

3.1.3.2 E-business registry service

Justification for inclusion and usage

Defines the set of services for centrally publishing, accessing and managing business information used in the trade community.

Standards for future consideration

Standard(s)	Description
ebXML Registry Service Specification	<p>The ebXML Registry Services (RS) Specification is one of the specifications within the ebXML framework of specifications. It describes how to build Registry Services that provide client access to the information content in the ebXML Registry.</p> <p>ebXML RS v3.0 is the latest OASIS approved standard.</p> <p>While the ebXML RS forms part of the ISO 15000 standard, OASIS technical committees retain the responsibility for maintaining and advancing ebXML standards.</p>

3.1.3.3 Transport-neutral mechanisms to address Web Services and messages

Justification for inclusion and usage

Web Services Addressing provides transport-neutral mechanisms to address Web Services and messages. Web Services Addressing 1.0 - Core (WS-Addressing) specification enables messaging systems to support message transmission through networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner.

Standards for future consideration

Standard(s)	Description
WS-Addressing 1.0	<p>Web Services Addressing 1.0 - Core (WS-Addressing) defines two constructs, message addressing properties and endpoint references, that normalize the information typically provided by transport protocols and messaging systems in a way that is independent of any particular transport or messaging system.</p> <p>A Web Services endpoint is a (referenceable) entity, processor, or resource to which Web Services messages can be addressed.</p> <p>The specification defines a family of message addressing properties that convey end-to-end message characteristics including references for source and destination endpoints and message identity that allows uniform addressing of messages independent of the underlying transport.</p> <p>Web Services Addressing 1.0 - Core specification is a W3C recommendation.</p>

3.1.3.4 Grammar for expressing the capabilities, requirements, and general characteristics of entities in an XML Web Services-based system

Justification for inclusion and usage

The Web Services Policy Framework (WS-Policy) provides a flexible and extensible grammar for expressing the capabilities, requirements, and general characteristics of entities in an XML Web Services-based system. It defines a framework and a model for the expression of these properties as policies.

Standards for future consideration

Standard(s)	Description
WS-Policy 1.5	<p>Web Services Policy 1.5 - Framework defines a policy to be a collection of policy alternatives, where each policy alternative is a collection of policy assertions. Some policy assertions specify traditional requirements and capabilities that will ultimately manifest on the wire (e.g. authentication scheme, transport protocol selection). Other policy assertions have no wire manifestation yet are critical to proper service selection and usage (e.g. privacy policy, QoS characteristics). Web Services Policy 1.5 - Framework provides a single policy language to allow both kinds of assertions to be reasoned about in a consistent manner.</p> <p>Web Services Policy 1.5 - Attachment, defines two general-purpose mechanisms for associating policies with the subjects to which they apply; the policies may be defined as part of existing metadata about the subject or the policies may be defined independently and associated through an external binding to the subject.</p> <p>The specifications became W3C Recommendations in September 2007.</p>

3.1.4 Interoperability areas for future consideration – standards not matured yet

3.1.4.1 Intra-government workflow and business process management

Justification for inclusion and usage

Defines how to model the flow of information within and between applications to implement business processes, including support for human interaction in processes.

Analysis

Business process modeling and workflow enables public and private processes to be modeled and defined. For example, how participants interact to execute a process (orchestration), including support for sub-processes; how transactions are managed, including support for long running transactions; and exception handling.

Standards in this area are immature with the result that workflow and business process management solutions are mostly proprietary, implemented by particular products, and allow:

- business process designers and application developers to define and agree business processes and workflow;
- the business processes and workflow to be executed according to the agreed specification.

Workflow logic can be programmed into a business application without using third party products, with the use of functional integration standards.

Business processes can be divided into two broad categories:

- Public processes that are exposed to business partners, citizens and other governments – G2B, G2C and G2G;
- Private processes that are internal to Government – application integration.

In many cases, the overall operations of Government will depend on a combination of public and private processes.

Standards for future consideration

Standard(s)	Description
Business Motivation Model (BMM), Business Process Definition Metamodel (BPDM), Business Process Maturity Model (BPMM), Business Process Modeling Notation (BPMN)	A collection of business process management specifications are under development by Object Management Group (OMG). They include Business Motivation Model (BMM), Business Process Definition Metamodel (BPDM), Business Process Maturity Model (BPMM), Business Process Modeling Notation (BPMN), etc. Further information is available at http://www.omg.org/technology/documents/br_pm_spec_catalog.htm

Standard(s)	Description
<p>Web Services Business Process Execution Language (WS-BPEL)</p>	<p>The Web Services Business Process Execution Language Technical Committee (TC) was formed at OASIS in April 2003. IBM, Microsoft, BEA, Siebel and SAP submit the BPEL4WS v1.1 to the TC for standardization in May 2003. BPEL4WS represents a convergence of the ideas in the XLANG and WSFL specifications. Both XLANG and WSFL are superseded by the BPEL4WS specification. The name of the proposed standard was changed to WS-BPEL recently.</p> <p>Business processes can be described in two ways. Executable business processes model the actual behaviour of a participant in a business interaction. Business protocols, in contrast, use process descriptions that specify the mutually visible message exchange behaviour of each of the parties involved in the protocol, without revealing their internal behaviour. The process descriptions for business protocols are called abstract processes. WS-BPEL is meant to be used to model the behaviour of both executable and abstract processes.</p> <p>WS-BPEL provides a language for the formal specification of business processes and business interaction protocols. By doing so, it extends the Web Services interaction model and enables it to support business transactions. WS-BPEL defines an interoperable integration model that should facilitate the expansion of automated process integration in both the intra-corporate and the business-to-business spaces.</p> <p>WS-BPEL 2.0 became an OASIS standard in April 2007.</p>
<p>Web Services Choreography</p>	<p>W3C created a Web Services Choreography Working Group to address the ability to compose and describe the relationships between Web Services. Three documents, Web Services Choreography Requirements, Web Services Choreography Model Overview, and Web Services Choreography Description Language v1.0 is currently a W3C Candidate Recommendation.</p> <p>Web Services Choreography Requirements describes a set of requirements for Web Services choreography based around a set of representative use cases, as well as general requirements for interaction among Web Services.</p> <p>Web Services Choreography Model Overview provides an information model that describes the data and the relationships between them that is needed to define a choreography that describes the interactions between two or more participants in order to meet some useful purpose.</p> <p>The Web Services Choreography Description Language (WS-CDL) is an XML-based language that describes peer-to-peer collaborations of Web Services participants by defining, from a global viewpoint, their common and complementary observable behaviour; where ordered message exchanges result in accomplishing a common business goal.</p>

Standard(s)	Description
Business Process Specification Schema (BPSS)	<p>BPSS is part of the ebXML framework. It provides a standard framework by which business systems may be configured to support execution of business collaborations consisting of business transactions. It is based upon prior UN/CEFACT work, specifically the metamodel behind the UN/CEFACT Modeling Methodology (UMM) defined in the N090R9.1 specification.</p> <p>The Specification Schema supports the specification of Business Transactions and the choreography of Business Transactions into Business Collaborations. Each Business Transaction can be implemented using one of many available standard patterns. These patterns determine the actual exchange of Business Documents and business signals between the partners to achieve the required electronic commerce transaction.</p> <p>The ebXML BPSS (ebBP) v2.0.4 became an OASIS standard in January 2007. This version of the ebBP technical specification addresses Business Collaborations between any number of parties (Business Collaborations specialized to Binary or Multiparty Collaborations). It also enables participants, which are capable of using Web Services or combined technologies (such as ebXML and Web Services) to participate in a Business Collaboration. It is anticipated that a subsequent version of this technical specification will address additional features such as the semantics of economic exchanges and contracts, and context-based content based on the metadata requirements provided by relevant organizations.</p>

3.1.4.2 Portable virtual machine package

Justification for inclusion and usage

Defines a standard, portable virtual machine package containing all required installation and configuration parameters for the distribution of virtual machines to and between virtualization platforms.

Analysis

A standard and portable virtual machine format enables the interoperability between different virtualization platforms. All required installation and configuration parameters are included in the package so that the virtual machines can be correctly installed and run in different virtualization platforms.

Standards for future consideration

Standard(s)	Description
Open Virtual Machine Format (OVF)	<p>OVF is a specification submitted by leading virtualization companies targeting an industry standard format for portable virtual machines. The companies behind the collaboration on this specification include Dell, HP, IBM, Microsoft, VMware, and XenSource.</p> <p>OVF uses existing packaging tools to combine one or more virtual machines together with a standards-based XML wrapper, giving the virtualization platform a portable package containing all required installation and configuration parameters for the virtual machines. This allows any virtualization platform that implements the standard to correctly install and run the virtual machines.</p> <p>OVF supports integrity checking of the virtual machines and provides mechanisms for license checking. OVF also allows an installed VM to acquire information about its host and run-time environment for application localization and performance optimization.</p> <p>The draft specification of OVF v0.9 was accepted by the Distributed Management Task Force (DMTF) in September 2007. OVF v1.0 is expected to be finalized in 2008.</p>

3.1.4.3 IT service modeling

Justification for inclusion and usage

Defines portable XML schema used to model complex IT services and systems, including their structure, constraints, policies, and best practices.

Analysis

The modeling enables a hierarchy of IT resource models to be created from reusable building blocks rather than requiring custom descriptions of every service, thus reducing costs and system complexity for customers.

Standards for future consideration

Standard(s)	Description
Service Modeling Language (SML)	<p>SML is an XML-based specification that defines a consistent way to express how computer networks, applications, servers and other IT resources are described or modeled so businesses can more easily manage the services that are built on these resources.</p> <p>It provides a rich set of constructs for creating models of complex IT services and systems. These models typically include information about configuration, deployment, monitoring, policy, health, capacity planning, target operating range, service level agreements, and so on.</p> <p>SML 1.1 is currently a W3C Working Draft.</p>

3.2 INFORMATION ACCESS AND INTERCHANGE DOMAIN

3.2.1 Interoperability areas for immediate consideration

3.2.1.1 Hypertext Web content

Justification for inclusion and usage

Development and formatting of hypertext documents for presentation on browsers via a range of delivery channels.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
HTML and XHTML	HTML and XHTML implemented by commonly adopted versions of browsers	None
Remarks: The content providers and application developers should state on their Web page how the content can best be viewed. They are also recommended to test their content against the prevailing versions of popular browsers such as Microsoft Internet Explorer and Mozilla Firefox.		

Recommended standards

Standard 1 HTML and XHTML implemented by commonly adopted versions of browsers	
Description	HTML (Hypertext Markup Language) 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. W3C describes XHTML (eXtensible Hypertext Markup Language) as “a reformulation of HTML v4.01 as an application of the eXtensible Markup Language (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.
Rationale for selection	Both HTML and XHTML are formal recommendations by the World Wide Web Consortium and are supported by the major browsers.
Maturity	Both HTML and XHTML are mature standards – the latest version of HTML (v4.01) was recommended by W3C in December 1999, and XHTML (v1.0) was recommended by W3C in January 2000.
Forward outlook	The HTML Workgroup of W3C will provide editorial revisions and bug fixes to HTML. In April 2001, W3C published Modularization of XHTML as a W3C Recommendation, as a means of subsetting and extending XHTML to extend the reach of XHTML to multiple platforms and devices. This was followed in May 2001 with the publication of XHTML 1.1 - Module-based XHTML. This specification is designed to be the basis for future extended XHTML Family document types. XHTML 2.0 is a next generation mark-up language. In this version, the functionality is expected to remain similar to (or a superset of) that of XHTML 1.1. However, the markup language may be altered semantically and syntactically to conform to the requirements of related XML standards such as XML Linking and XML Schema. The objective of these changes is to ensure

Standard 1 HTML and XHTML implemented by commonly adopted versions of browsers	
	<p>that XHTML 2.0 can be readily supported by XML browsers that have no arcane knowledge of HTML semantics such as linking, image maps, forms, etc. The development of XHTML 2.0 will likely require the development of new XHTML modules or revisions to existing XHTML modules.</p> <p>XHTML 2.0 is currently a W3C working draft http://www.w3.org/TR/xhtml2/.</p>
Version and rationale for version	<p>HTML and XHTML implemented by commonly adopted versions of browsers.</p> <p>HTML v4.01 is the current version of HTML. However, the major browsers implement some features differently and provide non-standard extensions.</p> <p>As there is a growing trend to adopt XHTML, it is recommended that only those features of HTML that are supported by XHTML are used.</p> <p>XHTML v1.0 is designed to reproduce HTML in XML. Reference should be made to the W3C's HTML Compatibility Guidelines (see http://www.w3c.org/TR/xhtml1/#guidelines) which provides guidelines for content authors developing XHTML to be rendered on existing HTML browsers. The W3C also provides a Validation Service (see http://validator.w3.org) to verify conformance to W3C specifications, including HTML and XHTML, as well as a list of tools to verify Web accessibility (see http://www.w3.org/WAI/ER/tools/Overview). Third party (see http://www.webstandards.org/) has also provided information to identify Web page rendering flaws in browsers.</p>
Limitations on the use of this standard	<p>The major browsers implement some features of HTML v4.01 differently and provide non-standard extensions. It is strongly recommended that content authors test compatibility of their content against the prevailing versions of popular browsers such as Microsoft Internet Explorer and Mozilla Firefox and consult the appropriate vendor documentation which discusses restrictions and deviations from the specifications.</p> <p>Government Web masters should monitor industry trends to determine which browser versions are being used by the public to ensure that testing is performed against those versions.</p> <p>Web masters should also state on their web page how the content can best be viewed.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.2 Client-side scripting**Justification for inclusion and usage**

Enables user interface functionality to be controlled programmatically to add interactivity and program logic to browser-based content e.g. to respond to a user's mouse action with the execution of program to validate user input.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
ECMA 262 Script	ECMA 262 Script 3 rd Edition	None

Recommended standards

Standard 1 ECMA 262 Script 3 rd Edition	
Description	ECMAScript is a standard script language, developed with the co-operation of Netscape and Microsoft and mainly derived from Netscape's JavaScript. Microsoft states that its latest version of JScript is the first implementation of the ECMAScript standard. Having the ECMAScript standard will help ensure more consistency between Netscape, Microsoft, and any other Web script implementations.
Rationale for selection	ECMA 262 is a well-recognised industry standard with support by the dominant browsers. There are no alternative candidate standards.
Maturity	The development of this Standard started in November 1996. The first edition of this ECMA Standard was adopted by the ECMA General Assembly of June 1997. The 3rd Edition of ECMA-262 was adopted by the ECMA General Assembly in December 1999.
Forward outlook	Work on the language is not complete. The technical committee is working on significant enhancements, including mechanisms for scripts to be created and used across the Internet, and tighter co-ordination with other standards bodies such as groups within the World Wide Web Consortium and the Wireless Application Protocol Forum. A conforming implementation of ECMA Script is permitted to provide additional types, values, objects, properties, and functions beyond those described in the 3 rd edition. In particular, a conforming implementation of ECMA Script is permitted to provide properties not described in this edition, and values for those properties, for objects that are described in the 3 rd edition.
Version and rationale for version	3 rd Edition is the current version and is supported by the popular browsers.
Limitations on the use of this standard	It is strongly recommended that content authors test compatibility of their scripts with different combinations of browser and operating system. Government web masters should also monitor industry trends to determine which browser versions are being used by the public to ensure that testing is performed against those versions.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.3 Mobile Web content

Justification for inclusion and usage

Formatting of content for presentation on mobile devices.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
WML HTML and XHTML XHTML Mobile Profile	WML 1.3 – for use with WAP devices HTML and XHTML as implemented by commonly adopted browsers on mobile devices – for use with mini-browsers XHTML Mobile Profile v1.1 – for use with mini-browsers on resource-constrained devices such as mobile phones	None
Remarks: Content authors are recommended to test their content against different popular browsers.		

Recommended standards

Standard 1 Wireless Mark-up Language (WML) v1.3	
Description	WML (Wireless Markup Language) is a language that allows the text portions of Web pages to be presented on mobile telephones and personal digital assistants (PDAs) via wireless access. WML is part of the Wireless Application Protocol (WAP).
Rationale for selection	WML is a 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). WML v1.3 is supported by microbrowsers from the leading microbrowser vendors.
Maturity	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 v1.3 was approved in July 2000. (Note that since 12 June 2002, a new group, the Open Mobile Alliance, controls WAP standards http://www.openmobilealliance.org/pr2002-06-12.html)

Standard 1 Wireless Mark-up Language (WML) v1.3	
Forward outlook	<p>The WAP Forum released the v2.0 of the WAP specification in August 2001. WML v2.0, part of the specification, is based on XHTML with WML v1.0 extensions to provide backward compatibility. WAP v2.0 also includes the XHTML Mobile Profile, based on the W3C's XHTML Basic specification with WAP extensions.</p> <p>WML v2.0 is intended for backward compatibility only and not for general authoring use. WAP2 content is to be created using the XHTML Mobile Profile.</p> <p>XHTML Mobile Profile is the official mark-up language of WAP 2.0 created by the Open Mobile Alliance (OMA) (formerly the WAP Forum) and will replace WML.</p>
Version and rationale for version	<p>Versions 1.3, which is the version supported by the leading microbrowser vendors.</p> <p>WML 1.3 forms part of the specification of WAP 1.2.1 and WAP 2.0.</p>
Limitations on the use of this standard	None.

Standard 2 HTML and XHTML as implemented by commonly adopted browsers on mobile devices
Please refer to the area "Hypertext Web Content" for details on HTML and XHTML

Standard 3 XHTML Mobile Profile v1.1	
Description	XHTML Mobile Profile is a document type based on the module framework and the modules defined by Modularization of XHTML. It is designed for resource-constrained Web clients that do not support the full set of XHTML features. Such resource-constrained devices can be such as mobile phones, PDAs, pagers and set-top boxes, etc.
Rationale for selection	XHTML Mobile Profile is supported by many mobile device browsers.
Maturity	XHTML Mobile Profile is the official mark-up language of WAP 2.0 first released by the Open Mobile Alliance (OMA) (formerly the WAP Forum) in October 2001.
Forward outlook	XHTML Mobile Profile will continue to be developed by the Open Mobile Alliance.
Version and rationale for version	Version 1.1, which is the current version and is widely supported. Version 1.1 was released by OMA in Sep 2002. This version has support for a scripting environment.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.4 Document file type for content publishing

Justification for inclusion and usage

Required to support the publishing of content e.g. a word processing document, spreadsheet, presentation etc. in read-only format, where the originator can provide a free viewer, or refer the receiver to a free viewer provided by a third party.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
HTML and XHTML PDF	HTML and XHTML as implemented by commonly adopted versions of browsers PDF	None
<p>Remarks:</p> <p>The HTML content providers should state on their document how the content can best be viewed. They are also recommended to test their contents against the prevailing versions of popular browsers such as Microsoft Internet Explorer and Mozilla Firefox.</p> <p>The PDF content providers should indicate which viewer software the recipients can use and supply a link to the viewer software if necessary.</p>		

Recommended standards

Standard 1 HTML and XHTML implemented by commonly adopted versions of browsers
Please refer to the area “Hypertext Web content” for details on HTML and XHTML

Standard 2 Portable Document Format (PDF)	
Description	PDF (Portable Document Format) is a file format that captures all of the elements of a printed document as an electronic image that you can view, navigate, print, or forward to someone else.
Rationale for selection	Format for document publishing from Adobe which is extensively used on the Internet. Supported by freely available Acrobat Reader and browser plug-ins.
Maturity	Version 1.2 was released in 1996. Version 1.3 was released in early 1999. Version 1.4 was released in 2001. Version 1.5 was released in 2003. Version 1.6 was released in late 2004. Version 1.7 was released in 2006 and ratified as ISO 32000 Part 1 in July 2008.
Forward outlook	PDF is likely to remain as an extensively used publishing format.
Version and rationale for version	Any version of PDF can be used in this area. The content providers should indicate which viewer software the recipients can use and supply a link to the viewer software if necessary.

Standard 2 Portable Document Format (PDF)	
Limitations on the use of this standard	None if purely for document publishing / viewing. While most viewers could render Chinese characters (including HKSCS) in PDF files, support for processing (e.g. copy and paste to other application) of Chinese characters in PDF file depends on both the viewer and the generator with which the PDF file is created.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.5 Document file type for receiving documents under ETO

Justification for inclusion and usage

Required to support the processing of electronic documents submitted pursuant to the ETO.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
.txt	.txt	None
.rtf	.rtf v1.6	
HTML	HTML	
PDF	PDF v1.2, 1.3, 1.4, 1.5, 1.6 or 1.7 (ISO 32000-1)	
Remarks: For HTML file types, members of the public should use only those HTML features that are implemented in common by Microsoft Internet Explorer 6/7 and Mozilla Firefox 2.0.x/3.0.x.		

Recommended standards

Standard 1 .txt	
Description	Plain/unformatted text files.
Rationale for selection	<i>De facto</i> standard for plain/unformatted text extensively supported by word processing packages, publishing tools, content management applications, e-mail applications etc.
Maturity	Mature.

Standard 1 .txt	
Forward outlook	Will continue to be supported as a common format.
Version and rationale for version	Not applicable. There is only one version of txt format.
Limitations on the use of this standard	No formatting and graphics can be retained.

Standard 2 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 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.
Rationale for selection	RTF is a <i>de facto</i> standard for text and graphics interchange and is available in the public domain. RTF is mature and well supported by all of the market leading word processing packages.
Maturity	Very mature. RTF version 1.6 was published in May 1999.
Forward outlook	RTF will continue to be developed by Microsoft to ensure support of new controls introduced in future versions of Microsoft Word for Windows and Macintosh platforms.
Version and rationale for version	RTF version 1.6 provides support for all control words introduced by Microsoft 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. Note that the version of RTF will be transparent to the public when they save documents in RTF format.
Limitations on the use of this standard	When documents are converted from a word processing format (e.g. .doc or .odt) 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”. 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. This is a known problem that cannot be solved currently.

Standard 3 HTML
Please refer to the area “Hypertext Web Content” for details on HTML and XHTML

Standard 4 Portable Document Format (.pdf) version 1.2, 1.3, 1.4, 1.5, 1.6 or 1.7 (ISO 32000-1)
Please refer to the area “Document file type for content publishing” for details on PDF

Standard 4 Portable Document Format (.pdf) version 1.2, 1.3, 1.4, 1.5, 1.6 or 1.7 (ISO 32000-1)	
Version and rationale for version	<p>PDF versions are explicitly specified in order to bound the acceptable versions so that B/Ds can have a stable configuration for processing electronic submissions and will not be affected by new PDF versions.</p> <p>The old versions of PDF are still acceptable in order to avoid forcing members of the public to upgrade their PDF generation software.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.6 Attachment of digital signature to electronic documents received under ETO

Justification for inclusion and usage

Required to support the attachment of digital signature to electronic documents submitted pursuant to the ETO.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
PKCS #7 S/MIME PDF RFC 3369	PKCS #7 v1.5 (RFC 2315) S/MIME v3 PDF v1.5, 1.6 or 1.7 (ISO 32000-1)	RFC 3369
Remarks: For electronic submissions via email pursuant to the ETO, members of the public should use only those S/MIME v3 features that are implemented in common by Microsoft Outlook Express 6.x and Mozilla Thunderbird v1.5 or above.		

Recommended standards

Standard 1 PKCS #7 v1.5 (RFC 2315)	
Description	PKCS #7, defined by RSA Security, defines a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.
Rationale for selection	<i>De facto</i> standard from RSA Security, PKCS#7 syntax is widely used in S/MIME v2 (native support), S/MIME v3 (backward compatible), and file-based signing / encrypting applications.
Maturity	PKCS #7 v1.5 is a mature standard defined in 1993. RFC 2315 was published by the IETF in March 1998.

Standard 1 PKCS #7 v1.5 (RFC 2315)	
Forward outlook	<p>In secure email, PKCS#7 v1.5 is supported in S/MIME v2 (native support) and S/MIME v3 (backward compatible). S/MIME v3, the dominant e-mail security standard, is based on RFC 3369.</p> <p>In file-based signing / encrypting applications, the migration from PKCS#7 to RFC 3369 is not noticeable. Therefore, PKCS #7 v1.5 will remain the standard for file-based cryptographic message syntax.</p>
Version and rationale for version	v1.5 is a mature standard and is supported by the file-based signing / encrypting applications.
Limitations on the use of this standard	None.

Standard 2 S/MIME (Secure Multi-purpose Internet Mail Extensions) v3	
Description	S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail with digital signature and encryption capability. It is included in the latest versions of the freely available email clients from Microsoft and Netscape and has also been endorsed by other vendors that make messaging products.
Rationale for selection	<p>S/MIME is a mature and well supported standard</p> <p>S/MIME is undergoing further development and is likely to remain the dominant standard to secure email.</p>
Maturity	<p>S/MIME v2 was published as an Informational RFC (RFC 2311 and 2312) in March 1998.</p> <p>S/MIME v3 was made an IETF standard (RFC 2630, 2632, 2633) in June 1999.</p> <p>IETF obsoleted RFC 2630 by RFC 3369 in August 2002 to include password-based key management, and an extension mechanism to support new key management schemes. The new RFC preserves backward compatibility with RFC 2630.</p> <p>The latest version, S/MIME v3.1, was made an IETF standard (RFC 3850-3852) in July 2004.</p>
Forward outlook	S/MIME is undergoing further development to incorporate support for new encryption standards and enhancements.
Version and rationale for version	<p>S/MIME v3 is recommended. However, different mail products may implement different sets of S/MIME v3 functions. Hence, the sender should be told what mail clients the receiver may be using so that the sender can avoid using those S/MIME v3 functions that are not supported by the receiver's mail clients.</p> <p>Meanwhile, the S/MIME v3 enabled Microsoft Outlook / Outlook Express v6.x and Mozilla Thunderbird v1.5 or above have become dominant in the user community.</p>
Limitations on the use of this standard	None.

Standard 3 PDF version 1.5, 1.6 or 1.7 (ISO 32000-1)	
Please refer to the area "Document file type for content publishing" for details on PDF	

Standard 3 PDF version 1.5, 1.6 or 1.7 (ISO 32000-1)	
Rationale for selection	A PDF file signed according to RFC 3778 makes use of well established open standards for digital signing, it is therefore considered acceptable as having a valid signature for submission under ETO when the whole document is signed.

Emerging standards for future consideration

Emerging Standard(s)	Description
RFC 3369	RFC 3369 is a proposed IETF standard published in 2002. It defines a standard to digitally sign, digest, authenticate or encrypt arbitrary messages. S/MIME v3 relies on RFC 3369.

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.7 Formatted document file type for collaborative editing

Justification for inclusion and usage

Format for the interchange of formatted documents that need to be edited collaboratively by a user community.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
.rtf HTML .doc .odt ISO/IEC DIS 29500 (Office Open XML)	.rtf v1.6 HTML and XHTML as implemented by commonly adopted versions of browsers .doc (Word 97 file format which is used by Word 97 and later versions) .odt (OpenOffice.org v2.0 file format based on OpenDocument 1.0)	ISO/IEC DIS 29500 (Office Open XML)
<p>Remarks:</p> <p>If the sender is uncertain what office software the recipients are using, the sender should send the documents in a format (e.g. .htm, .rtf, .doc) that common office software available in the market are able to handle. However, if both sides are using office software that belong to the same family, then tool-specific format like .sxw may be used for file exchange.</p> <p>For HTML documents, the sender is also recommended to test their content against the prevailing versions of popular browsers such as Microsoft Internet Explorer and Mozilla Firefox.</p> <p>B/Ds should refer to OGCIO Circular No. 5/2006 (Guidelines for exchanging electronic documents) for guidelines on how to reduce their exposure to incompatibility problems arising from the mixed use of different office software products or different versions of the same product in a user community.</p>		

Recommended standards

Standard 1 Rich Text Format (.rtf) v1.6
Please refer to the area “Document file type for receiving documents under ETO” for details on rtf v1.6.

Standard 2 HTML and XHTML implemented by commonly adopted versions of browsers
Please refer to the area “Hypertext Web content” for details on HTML and XHTML.

Standard 3 .doc (Word 97 file format which is used by Word 97 and later versions)	
Description	Proprietary Microsoft Word document format used by Microsoft Word 97 and later versions.
Rationale for selection	Commonly used document format. Also supported by open source alternatives.
Maturity	Mature.
Forward outlook	Microsoft Word is likely to remain one of the major word processing applications in the near future. Microsoft has announced that the next version of Word will use an XML-based file format by default. Nevertheless, the binary formats (.doc, .ppt and .xls) will still be available in the next version of Office.
Version and rationale for version	Different versions of Word are used within and outside the government and there are incompatibilities between these versions. Word 97 file format should be treated as the file format for exchange as later versions share the same file format.
Limitations on the use of this standard	New features that are provided in newer version(s) of Microsoft Office may not be supported in the older version(s). Please refer to the following web pages for more information: http://www.microsoft.com/technet/prodtechnol/office/office2003/operate/o03fls/hr.msp http://www.microsoft.com/technet/prodtechnol/office/officexp/maintain/filesar.msp

Standard 4 .odt (OpenOffice.org v2.0 file format based on OpenDocument 1.0)	
Description	The .odt format is the default document format for OpenOffice.org v2.0 or later. It is a new document format introduced in the OpenOffice.org v2.0. It is based on the OpenDocument 1.0 (an open standard ratified by the OASIS in May 2005), but it uses its own specific file extension. OpenDocument is made up of a single XML schema for text, spreadsheets, charts and graphical documents. It makes use of the existing standards, such as HTML, SMIL (Synchronized Multimedia Integration Language) and XForms, and is designed so that it can be used as a default file format for different office applications.

Standard 4 .odt (OpenOffice.org v2.0 file format based on OpenDocument 1.0)	
Rationale for selection	<p>The .odt format is expected to be compatible with other document formats which conform to OpenDocument 1.0. It has been gaining increasing support from the open source vendors. The .odt format is for use in document interchange between users of OpenOffice.org v2.0 or its variants.</p> <p>OpenDocument is an open standard and designed to be used by different office applications. As comparing with other proprietary document formats, OpenDocument is less vulnerable to such problems as format incompatibility and obsolescence. The .odt format is the default file format in the open-source office suite OpenOffice.org v2.0 and also other OpenOffice variants such as StarOffice 8.0.</p>
Maturity	<p>Since its debut in October 2000, the OpenOffice.org has been improving on its functions and features under the leadership of an open source community. The OpenOffice.org v2.0 was published in October 2005 and it has been well received by the user community.</p>
Forward outlook	<p>.odt is envisaged to gain extensive use among the users of OpenOffice.org or its variants.</p>
Version and rationale for version	<p>Currently, only one version of .odt exists.</p>
Limitations on the use of this standard	<p>If the implementations of OpenOffice.org v2.0 products conform to the OpenOffice.org v2.0 specifications for extensions to the OpenOffice.org v2.0 file format (e.g. to support Chinese characters), interoperability across these variants will be enhanced. It is recommended that conformance be verified during product selection.</p> <p>Earlier versions of OpenOffice.org do not support this new format but converting the documents back to older versions could be done as circumvention. However, new features are not supported by old versions. There is no perfect solution for the issue.</p> <p>Microsoft does not support the standard for the time being and there is no known plan for such support in its Microsoft Office product suite.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
ISO/IEC DIS 29500 (Office Open XML)	<p>Office Open XML (OOXML) is the default file format of Office 2007, which is different from the default format adopted in previous versions of the software suite.</p> <p>OOXML was approved as an Ecma standard (Ecma 376) in December 2006. It was submitted to ISO and became the ISO/IEC DIS 29500 Draft International Standard. It has received the necessary number of votes for approval as an ISO/IEC International Standard after the ballot resolution meeting held in February 2008. However, ISO announced on 6 June 2008 that four participating countries of ISO and IEC – Brazil, India, South Africa and Venezuela – have submitted appeals against the approval of ISO/IEC DIS 29500 as an ISO/IEC International Standard. On 15 August 2008, ISO announced the DIS 29500 (Office Open XML) could proceed to publication as an ISO/IEC International Standard after appeals by four national standards bodies against the approval of the document failed to garner sufficient support.</p> <p>It is observed that products that can fully support the ISO/IEC DIS 29500 (Office Open XML) standard are not yet available.</p>

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.8 Presentation file type for collaborative editing

Justification for inclusion and usage

Format for the interchange of presentation files that need to be edited collaboratively by a user community.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
.ppt .odp ISO/IEC DIS 29500 (Office Open XML)	.ppt (PowerPoint 97 file format which is used by PowerPoint 97 and later versions) .odp (OpenOffice.org v2.0 file format based on OpenDocument 1.0)	ISO/IEC DIS 29500 (Office Open XML)
<p>Remarks:</p> <p>If the sender is uncertain what office software the recipients are using, the sender should send the presentation in a format (e.g. .ppt) that common office software available in the market are able to handle. However, if both sides are using office software that belong to the same family, then tool-specific format like .sxi may be used for file exchange.</p> <p>B/Ds should refer to OGCIO Circular No. 5/2006 (Guidelines for exchanging electronic documents) for guidelines on how to reduce their exposure to incompatibility problems arising from the mixed use of different office software products or different versions of the same product in a user community.</p>		

Recommended standards

Standard 1 .ppt (PowerPoint 97 file format which is used by PowerPoint 97 and later versions)	
Description	Proprietary Microsoft presentation format used by Microsoft PowerPoint 97 and later versions.
Rationale for selection	Commonly used presentation format. Also supported by open source alternatives.
Maturity	Mature.
Forward outlook	Microsoft PowerPoint is likely to remain as one of the major players for presentation application in the near future. Microsoft has announced that the next version of PowerPoint will use an XML-based file format by default. Nevertheless, the binary formats (.doc, .ppt and .xls) will still be available in the next version of Office.
Version and rationale for version	Different versions of PowerPoint are used within and outside the Government and there are incompatibilities between these versions. PowerPoint 97 file format should be treated as the file format for exchange as later versions of PowerPoint share the same file format.

Standard 1 .ppt (PowerPoint 97 file format which is used by PowerPoint 97 and later versions)	
Limitations on the use of this standard	<p>New features that are provided in newer version(s) of Microsoft Office may not be supported in the older version(s). Please refer to the following web pages for more information:</p> <p>http://www.microsoft.com/technet/prodtechnol/office/office2003/operate/o03flshr.mspx</p> <p>http://www.microsoft.com/technet/prodtechnol/office/officexp/maintain/filesहार.mspx</p>

Standard 2 .odp (OpenOffice.org v2.0 file format based on OpenDocument 1.0)	
Description	The .odp format is the default presentation format for OpenOffice.org v2.0 or later. It is a new presentation format introduced in the OpenOffice.org v2.0. It is based on the OpenDocument 1.0 (an open standard ratified by the OASIS), but it uses its own specific file extension.
Rationale for selection	The .odp format is expected to be compatible with other document formats which conform to OpenDocument 1.0. It has been gaining increasing support from the open source vendors. The .odp format is for use in document interchange between users of OpenOffice.org v2.0 or its variants.
Maturity	Since its debut in October 2000, the OpenOffice.org has been improving on its functions and features under the leadership of an open source community. The OpenOffice.org v2.0 was published in October 2005 and it has been well received by the user community.
Forward outlook	.odp is envisaged to gain extensive use among the users of OpenOffice.org or its variants.
Version and rationale for version	Currently, only one version of .odp exists.
Limitations on the use of this standard	<p>If the implementations of OpenOffice.org v2.0 products conform to the OpenOffice.org v2.0 specifications for extensions to the OpenOffice.org v2.0 file format (e.g. to support Chinese characters), interoperability across these variants will be enhanced. It is recommended that conformance be verified during product selection.</p> <p>Earlier versions of OpenOffice.org do not support this new format but converting the documents back to older versions could be done as circumvention. However, new features are not supported by old versions. There is no perfect solution for the issue.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
ISO/IEC DIS 29500 (Office Open XML)	Please refer to the area "Formatted document file type for collaborative editing" for details on the ISO/IEC DIS 29500 (Office Open XML) format.

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.9 Spreadsheet file type for collaborative editing

Justification for inclusion and usage

Format for the interchange of spreadsheets that need to be edited collaboratively by a user community

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
.xls .ods ISO/IEC DIS 29500 (Office Open XML)	.xls (Excel 97 file format which is used by Excel 97 and later versions) .ods (OpenOffice.org v2.0 file format based on OpenDocument 1.0)	ISO/IEC DIS 29500 (Office Open XML)
<p>Remarks:</p> <p>If the sender is uncertain what office software the recipients are using, the sender should send the spreadsheet in a format (e.g. .xls) that common office software available in the market are able to handle. However, if both sides are using office software that belong to the same family, then tool-specific format like .sxc may be used for file exchange.</p> <p>B/Ds should refer to OGCIO Circular No. 5/2006 (Guidelines for exchanging electronic documents) for guidelines on how to reduce their exposure to incompatibility problems arising from the mixed use of different office software products or different versions of the same product in a user community.</p>		

Recommended standards

Standard 1 .xls (Excel 97 file format which is used by Excel 97 and later versions)	
Description	Proprietary Microsoft spreadsheet format used by Microsoft Excel 97 and later versions.
Rationale for selection	Commonly used spreadsheet format. Also supported by open source alternatives.
Maturity	Mature.
Forward outlook	Microsoft Excel is likely to remain as one of the major spreadsheet applications in the near future. Microsoft has announced that the next version of Excel will use an XML-based file format by default. Nevertheless, the binary formats (.doc, .ppt and .xls) will still be available in the next version of Office.
Version and rationale for version	Different versions of Excel are used within and outside the Government and there are incompatibilities between these versions. Excel 97 file format should be treated as the file format for exchange as later versions share the same file format.
Limitations on the use of this standard	New features that are provided in newer version(s) of Microsoft Office may not be supported in the older version(s). Please refer to the following web pages for more information: http://www.microsoft.com/technet/prodtechnol/office/office2003/operate/o03flshr.mspx http://www.microsoft.com/technet/prodtechnol/office/officexp/maintain/fileshar.mspx

Standard 2 .ods (OpenOffice.org v2.0 file format based on OpenDocument 1.0)	
Description	The .ods format is the default spreadsheet format for OpenOffice.org v2.0 or above. It is a new spreadsheet format introduced in the OpenOffice.org v2.0. It is based on the OpenDocument 1.0 (an open standard ratified by the OASIS), but it uses its own specific file extension.
Rationale for selection	The .ods format is expected to be compatible with other document formats which conform to OpenDocument 1.0. It has been gaining increasing support from the open source vendors. The .ods format is for use in document interchange between users of OpenOffice.org v2.0 or its variants.
Maturity	Since its debut in October 2000, the OpenOffice.org has been improving on its functions and features under the leadership of an open source community. The OpenOffice.org v2.0 was published in October 2005 and it has been well received by the user community.
Forward outlook	.ods is envisaged to gain extensive use among the users of OpenOffice.org or its variants.
Version and rationale for version	Currently, only one version of .ods exists.
Limitations on the use of this standard	<p>If the implementations of OpenOffice.org v2.0 products conform to the OpenOffice.org v2.0 specifications for extensions to the OpenOffice.org v2.0 file format (e.g. to support Chinese characters), interoperability across these variants will be enhanced. It is recommended that conformance be verified during product selection.</p> <p>Earlier versions of OpenOffice.org do not support this new format but converting the documents back to older versions could be done as circumvention. However, new features are not supported by old versions. There is no perfect solution for the issue.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
ISO/IEC DIS 29500 (Office Open XML)	Please refer to the area "Formatted document file type for collaborative editing" for details on the ISO/IEC DIS 29500 (Office Open XML) format.

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.10 E-mail format

Justification for inclusion and usage

Required to enable e-mail exchange.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
MIME	MIME (RFCs 2045, 2046, 2047, 2048, 2049, 2231, 2387, 2392, 2557, 2646, 3023)	None

Recommended standards

Standard 1 Multipurpose Internet Mail Extensions (MIME) (RFCs 2045, 2046, 2047, 2048, 2049, 2231, 2387, 2392, 2557, 2646, 3023)	
Description	MIME (Multi-Purpose Internet Mail Extensions) is an extension of the SMTP protocol that enables the exchange of different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII handled in the original protocol. It thus addresses the problems associated with RFCs 2821 and 2822.
Rationale for selection	Globally recognised, mature IETF standard. Complementary to SMTP.
Maturity	MIME standard RFCs 1521 and 1522 were created in September 1993. They were subsequently obsoleted by RFCs 2045, 2046, 2047, 2048 and 2049 published in 1996 and complemented by RFCs 2231 published in 1997, 2646 published in 1999 and 3023 published in January 2001.
Forward outlook	MIME has been carefully designed as an extensible mechanism, and it is expected that the set of content-type/subtype pairs and their associated parameters will grow significantly with time. Several other MIME fields, notably including character set names, are likely to have new values defined over time. In order to ensure that the set of such values is developed in an orderly, well-specified, and public manner, MIME defines a registration process which uses the Internet Assigned Numbers Authority (IANA) as a central registry for such values.
Version and rationale for version	The version of MIME is as defined in RFCs 2045, 2046, 2047, 2048, 2049, 2231, 2387, 2392, 2557, 2646, 3023.
Limitations on the use of this standard	None

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.11 E-mail security

Justification for inclusion and usage

Required to support the security of messages which may include authenticity and integrity as well as confidentiality. E-mail products must support interfaces that conform to the e-mail security standards for sending secure messages.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
S/MIME PGP PEM MIME Object Security Services	S/MIME v3	None
<p>Remarks:</p> <p>For electronic submissions via email pursuant to the ETO, members of the public should use only those S/MIME v3 features that are implemented in common by Microsoft Outlook Express 6.x and Mozilla Thunderbird v1.5 or above.</p>		

Recommended standards

Standard 1 S/MIME (Secure Multi-purpose Internet Mail Extensions) v3
Please refer to the area “Attachment of digital signature to electronic documents received under ETO” for details on S/MIME.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
Pretty Good Privacy (PGP)	<p>Free software is available.</p> <p>However, the distribution of the necessary keys to large user groups is difficult to manage securely, and so this limits the size of the user community built around PGP implementations and therefore PGP is usually regarded as a solution for small e-mail communities – and is therefore inappropriate for use by Government. The extent of adoption of PGP indicates that, once the key distribution problem has been resolved, PGP provides acceptable e-mail security. Although the longest established standard in this area, PGP is, however, no longer supported by its original developers.</p> <p>While difficult to manage certificates across large user communities, PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations.</p>
Privacy Enhanced Mail (PEM) MIME Object Security Services	Two standards, PEM and MIME Object Security Services, have both been proposed for developing e-mail, but neither has been widely used.

3.2.1.12 Graphical / Image File Types

Justification for inclusion and usage

Formatting of graphics and images, including simple animation, for interchange between bureaux and departments and/or third parties.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
.jpg .gif .tif .bmp .png .epsf .tga	.jpg – for images that will tolerate information loss .gif v89a - for images that will tolerate information loss with few colours and limited graduation between colours .tif v6 - good for images that will not tolerate information loss .png (second edition) - as an alternative to gif v89a offering greater compression and where control over transparency is required epsf v3 – for images that require editing and/or which are included in PostScript printed output	None

Recommended standards

Standard 1 .jpg	
Description	Joint Photographic Experts Group (JPEG) is an ISO graphic image file format standard (ISO 10918).
Rationale for selection	Widely supported by browsers and the majority of image processing, graphics design, photo processing and scanner accessory software.
Maturity	Mature. Originally ratified in 1994. Natively supported by Netscape Navigator and Internet Explorer since version 2.
Forward outlook	Work has been underway on JPEG-2000. Part 1 (the core) was published as International standard, parts 2-6 are complete or nearly complete, and parts 8-11 are under development.
Version and rationale for version	JPEG as defined by ISO standard 10918. This is the current version of the ISO published standard and is widely supported by appropriate products.
Limitations on the use of this standard	None.

Standard 2 .gif v89a	
Description	Graphics Interchange Format (GIF) is one of the most common formats for graphics images on the Web.
Rationale for selection	Graphics Interchange Format is a <i>de facto</i> standard widely supported by browsers and the majority of image processing, graphics design, photo processing and scanner accessory software.
Maturity	Natively supported by Microsoft Internet Explorer since v3 and Netscape Navigator since v2.

Standard 2 .gif v89a	
Forward outlook	Will continue to be a widely supported graphic image file format. May be replaced by Portable Network Graphics format.
Version and rationale for version	Version 89a is the latest version.
Limitations on the use of this standard	None.

Standard 3 .tif v6	
Description	Tag Image File Format (TIFF) is a common format for exchanging raster graphics (bitmap) images between application programs.
Rationale for selection	Tagged Image File Format is a <i>de facto</i> standard of particular benefit for images that will not tolerate information loss.
Maturity	Mature. Version 6 was published in 1992.
Forward outlook	Will continue to be a widely supported graphic image file format.
Version and rationale for version	Version 6 is the current version, published in June 1992.
Limitations on the use of this standard	None.

Standard 4 .png (second edition)	
Description	Portable Network Graphics (PNG) is a widely supported image compression format
Rationale for selection	The specification was published initially by the IETF, recommended by the W3C and is reaching the final stages of ISO/IEC standardisation.
Maturity	Mature. PNG was first published by the IETF in 1997 and recommended by the W3C. Second edition (ISO/IEC 15948:2003) was recommended by W3C in November 2003.
Forward outlook	Portable Network Graphics format is expected to replace GIF as the dominant image compression format in use on the Internet.
Version and rationale for version	Second edition, the current version, which is widely supported by various products.
Limitations on the use of this standard	None.

Standard 5 epsf v3	
Description	Encapsulated PostScript File (EPSF) is a format for importing and exporting PostScript language files among applications. An Encapsulated PostScript file is a PostScript language program describing the appearance of a single page and is typically used for inclusion in another PostScript language page description.
Rationale for selection	EPSF is widely adopted in professional and academic publications (e.g. IEEE) as the accepted format for graphics.
Maturity	Mature. Version 3 of the specification was published by Adobe in 1992.
Forward outlook	EPSF is likely to remain a commonly used standard until vector graphics standards become sufficiently mature to replace it.

Standard 5 epsf v3	
Version and rationale for version	Version 3 published by Adobe in 1992 is the current specification. It is widely adopted in professional and academic publications.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
.bmp	Windows Bitmap (BMP) files are stored in a device-independent bitmap format that allows Windows to display the bitmap on any type of display device. BMP has not been selected as it does not offer the same levels of compression as GIF, TIFF or JPEG (when those standards are used appropriately) and thus is not appropriate for efficient and effective delivery of images via the Internet.
.tga	Truevision (Targa / TGA) file format is usually used in areas that require very high image qualities such as medical imaging. Professional graphics editing software such as Adobe PhotoShop supports the TGA format. Both TIFF, which is a recommended specification in the IF, and TGA offer lossless compression but TGA provides deeper colour depth than TIFF. However, TIFF is more widely supported than TGA in general office environment because office tools like Microsoft Word can import image files in TIFF format. TGA format files are very large and are more commonly used for niche high-end image processing applications.

3.2.1.13 Character sets and encoding for Web content

Justification for inclusion and usage

Defines the character sets and encoding to be used for Web content in English or Chinese.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
ISO/IEC 8859-1 ISO 10646 and HKSCS BIG-5 and HKSCS	ISO/IEC 8859-1:1998 – for encoding content in English ISO/IEC 10646-1:2000 and HKSCS-2001 – for encoding content in English or Chinese (Chinese characters are restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO 10646 standard and the HKSCS-2001) BIG-5 and HKSCS-2001 – for encoding content in Chinese	None

Remarks:

For the correct display of Web content, the content provider should specify the character encoding in the document explicitly.

ISO 10646 is the standard for the common Chinese language interface, B/Ds are recommended to adopt ISO 10646, where applicable.

The use of ISO/IEC 10646 standard (Unicode) for new Chinese version Web sites is specified in the “Guidelines on Dissemination of Information through Government Homepages, January 2008”, which is available at:

<http://www.ogcio.gov.hk/eng/knowledge/ech9-a.htm - ech9a> (Internet) or

<http://itginfo.ccgo.hksarg/content/isd/guideline/guidelines2008.pdf> (intranet).

The International Ideographs Core (IICORE), a subset of the ISO 10646 standard (comprising the most commonly used characters) designed for use on resource-limited devices, was published in the ISO 10646:2003 Amendment 1.

Recommended standards

Standard 1 ISO/IEC 8859-1:1998	
Description	ISO/IEC 8859-1 is a member of the ISO/IEC 8859 family of character codes which extend ASCII in different ways with different characters used in different languages and cultures. ISO/IEC 8859-1 contains ASCII characters and a collection of characters needed in western European languages.
Rationale for selection	ISO/IEC 8859-1 is commonly used for the publication of English language web page content
Maturity	ISO/IEC 8859 character sets were originally designed in the mid 1980s by the European Computer Manufacturers Association and were subsequently endorsed by ISO.
Forward outlook	ISO/IEC 8859-1 will coexist with ISO 10646. It is observed that many newly provisioned English Web pages are encoded in ISO 10646 standard. The ISO 10646 standard is recommended to encode English Web pages.
Version and rationale for version	ISO/IEC 8859-1:1998. Latest version published by ISO.
Limitations on the use of this standard	ISO/IEC 8859-1 is an 8-bit single-byte encoding scheme. Some characters under ISO/IEC 8859-1 use all 8 bits, and software designed to handle double byte characters, such as BIG-5, may misinterpret the full 8-bit ISO 8859-1 characters in conjunction with the characters that follow them as double byte characters, causing confusion and distortion. Content developers should test their content using multi-byte language (e.g. Chinese) Web browsers or equivalent rendering tools to ensure that content is not being misinterpreted.

Standard 2 BIG-5	
Description	<i>A de facto</i> standard for traditional Chinese characters.
Rationale for selection	Widely adopted in HK and Taiwan.
Maturity	An official code was announced in 1984.

Standard 2 BIG-5	
Forward outlook	<p>With effect from 31 March 2008, the Chinese Language Interface Advisory Committee (CLIAC) will continue to assign only ISO 10646 code points to newly included HKSCS characters. All HKSCS characters already assigned with code points before the effective date will not be affected. Further information is available at:</p> <p>http://www.ogcio.gov.hk/ccli/eng/hkscs/reviced_principles.html</p> <p>The last batch of HKSCS characters assigned with Big-5 code points has been published and is available at:</p> <p>http://www.ogcio.gov.hk/ccli/eng/hkscs/download/newchar.pdf</p>
Version and rationale for version	<p>The BIG-5 standard for the coding of Chinese characters promulgated by the Institute for Information Industry of Taiwan [Document reference and version: Computer Chinese Glyph and Character Code Mapping Table and Technical Report C-26 (May 1984)].</p>
Limitations on the use of this standard	<p>Big-5 encoded Web pages cannot include the HKSCS characters which are newly included after 31 March 2008.</p>

Standard 3 ISO/IEC 10646-1:2000	
Description	<p>ISO 10646 is an ISO standard to encode the characters of the major languages of the world into a single character set.</p> <p>ISO 10646 is code-for-code compatible with Unicode which can be considered an implementation of ISO 10646.</p> <p>Unicode can be encoded in different ways. UTF-8 is the most common way of encoding content that are based on the ISO 10646 standard.</p>
Rationale for selection	<p>ISO 10646 is widely supported by a broad range of products, including databases, fonts and printing tools, internationalisation libraries and office productivity tools.</p>
Maturity	<p>The first version of the ISO 10646 standard (i.e. ISO/IEC 10646-1:1993) was released in 1993.</p> <p>The latest version is ISO/IEC 10646:2003, which is a single publication as the result of the merger of the previous two releases of ISO 10646 standard: ISO/IEC 10646-1:2000 and ISO/IEC 10646-2:2001. The ideographic characters in the ISO/IEC 10646:2003 standard are the same as those in ISO/IEC 10646-1:2000 cum ISO/IEC 10646-2:2001.</p> <p>The ISO/IEC 10646:2003 Amendment 1 was published by ISO in November 2005. The progress of the release of new ISO/IEC 10646:2003 amendments is summarized at the following URL:</p> <p>http://www.ccli.gov.hk/tc_chi/info/info_iso3.html (Chinese version only).</p>
Forward outlook	<p>ISO 10646 is a fundamental standard and will continue to evolve.</p> <p>The IICORE contains the most commonly used ideographic characters of the ISO 10646. The definition of this subset is for use on resource-limited devices where implementation of the complete ISO 10646 ideograph repertoire would be cumbersome.</p> <p>The IICORE was also published in the ISO 10646:2003 Amendment 1. Further information about IICORE is available at:</p> <p>http://www.ogcio.gov.hk/ccli/eng/structure/iicore.html</p>

Standard 3 ISO/IEC 10646-1:2000	
Version and rationale for version	ISO/IEC 10646-1:2000 because product support for ISO/IEC 10646-1:2000 is mature and an increase in the product support for ISO/IEC 10646:2003 with Amendment 1 is noted, where ISO/IEC 10646:2003 with Amendment 1 includes the HKSCS-2004.
Limitations on the use of this standard	None.

Standard 4 HKSCS-2001	
Description	A local character set & encoding standard developed by the Government to provide support for the characters used within HKSAR which are not covered by other standards, such as BIG-5 and ISO 10646.
Rationale for selection	HKSCS is widely supported by Chinese software in HK.
Maturity	First published in 1999 and revised in 2001 and 2004. The latest version is the HKSCS-2004 released in May 2005, available at http://www.ogcio.gov.hk/ccli/eng/hkscs/introduction.html . The 4,941 characters in the HKSCS-2004 are included in the ISO 10646. The HKSCS-2004 has 123 more characters as compared to the HKSCS-2001.
Forward outlook	HKSCS will be continuously updated to cater for new characters. Results of the Inclusion of Characters in the HKSCS after the publication of the HKSCS-2004 is available at the following URL: http://www.ogcio.gov.hk/ccli/eng/hkscs/applcn.html A new version of HKSCS (tentatively named as HKSCS-2008) will be published.
Version and rationale for version	Product support for HKSCS-2001 is already mature.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.14 Character sets and encoding for other types of information exchange

Justification for inclusion and usage

Defines the character sets and encoding to be used for exchanging information in English or Chinese in general. For character sets and encoding for Web content, please refer to the previous interoperability area.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
ASCII ISO 10646 and HKSCS BIG-5 and HKSCS	ASCII – for encoding content in English ISO/IEC 10646-1:2000 and HKSCS-2001 – for encoding content in English or Chinese (Chinese characters are restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO 10646 standard and the HKSCS-2001) BIG-5 and HKSCS-2001 – for encoding content in Chinese	None
<p>Remarks:</p> <p>Where applicable (e.g. in XML documents), the content provider should specify the character encoding in the document explicitly (e.g. use <?xml encoding="UTF-8"?> to specify the UTF-8 encoding in an XML document).</p> <p>ISO 10646 is the standard for the common Chinese language interface, B/Ds are recommended to adopt ISO 10646, where applicable.</p> <p>The IICORE was also published in the ISO 10646:2003 Amendment 1. Further information about IICORE is available at: http://www.ogcio.gov.hk/ccli/eng/structure/iicore.html.</p> <p>Big-5 is not recommended for encoding newly provisioned Chinese content because the HKSCS characters newly included after 31 March 2008 will not be assigned with Big-5 code points.</p>		

Recommended standards

Standard 1 ASCII	
Description	ASCII (American Standard Code for Information Interchange) is the most common standard for coding textual content in English.
Rationale for selection	ASCII (ISO 646), developed by the American National Standards Institute, is the dominant standard for coding textual content in English.
Maturity	First published as ANSI X3.4 in 1968.
Forward outlook	Will coexist with ISO 10646 but will, possibly, in the long term, be replaced.
Version and rationale for version	There is only one version of ASCII.
Limitations on the use of this standard	None.

Standard 2 BIG-5
Please refer to the area “Character sets and encoding for Web content” for details on BIG-5

Standard 3 ISO/IEC 10646-1:2000
Please refer to the area “Character sets and encoding for Web content” for details on ISO/IEC 10646-1:2000

Standard 4 HKSCS-2001
Please refer to the area “Character sets and encoding for Web content” for details on HKSCS-2001

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.15 Compressed files

Justification for inclusion and usage

Defines the applications and format to be used for compressing files for interchange.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
.zip	.zip	.rar
.gz	.gz v4.3	
.rar		

Recommended standards

Standard 1 .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.
Rationale for selection	<i>De facto</i> standard for file compression.
Maturity	Mature. Introduced in 1989.
Forward outlook	Will continue to be a commonly utilised file compression format.
Version and rationale for version	Only one version available.
Limitations on the use of this standard	None.

Standard 2 .gz v4.3	
Description	GNU zip (gzip) is a compression utility. It has been adopted by the GNU project and is popular on the Internet.
Rationale for selection	Version 4.3 is an IETF standard (RFC 1952) and is popular on the Internet.
Maturity	Mature.
Forward outlook	Will continue to be a commonly utilised file compression format.

Standard 2 .gz v4.3	
Version and rationale for version	Version 4.3 is the current version. There have been no technical changes to the gzip format since version 4.1 of this specification. In version 4.2, some terminology was changed, and the sample CRC code was rewritten for clarity and to eliminate the requirement for the caller to do pre- and post-conditioning. Version 4.3 is a conversion of the specification to RFC style, and is documented in RFC 1952.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
.rar	Similar to the .zip format, .rar is an archiving format for storing one or more files in the compressed form. Currently, only the commercial software WinRAR can both create and extract .rar files while there are some free extraction-only tools available. There is a growing trend in using the .rar format, partly because of its good compression capability and function of disassembling a large archive into smaller sequenced parts that facilitates transmission over links of lower speed or with file size restriction imposed. However, the format is yet to become prevalent as compared with the .zip format.

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.16 Removable storage media for receiving documents under the ETO

Justification for inclusion and usage

Defines the media and format to be used for the interchange of information via removable storage media under ETO.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
3.5" 1.44 MB floppy diskette	3.5" 1.44 MB floppy diskette in MS-DOS format	None
CD-ROM	CD-ROM in ISO 9660:1988 format	
DVD-ROM	DVD-ROM in ISO/IEC 13346:1995 format	

Recommended standards

Standard 1 ISO 9660:1988	
Description	Specifies the volume and file structure of compact read-only optical disks (CD-ROM) for the information interchange between information processing systems. The specification defines the attributes of the volume and the descriptors recorded on it; the relationship among volumes of a volume set; the placement of files; the attributes of the files; recorded structures intended for input or output data streams of an application program when required to be organized as sets of records; three nested levels of medium interchange; two nested levels of implementation; requirements for the processes provided within information processing systems.
Rationale for selection	ISO 9660:1988 is a mature industry standard with almost universal support
Maturity	Mature. Published as an ISO standard in 1988.
Forward outlook	Will remain as the dominant file format for removable storage media
Version and rationale for version	ISO 9660:1988 is the published ISO standard
Limitations on the use of this standard	None

Standard 2 DVD-ROM ISO/IEC 13346:1995	
Description	ISO/IEC 13346:1995 specifies the volume and file structure of write-once and rewritable media using non-sequential recording for information interchange. This ISO standard is equivalent to ECMA 167 2nd edition. The prevalent file system structure of DVD-ROM (Universal Disk Format (UDF)) is based on the ISO/IEC 13346:1995 standard. With the lowering of its cost and that of access equipment, DVD-ROM has gained in popularity over the years. Besides, the DVD readers produced in recent years are often able to read different DVD recordable disc formats (i.e. DVD-RW, DVD-RAM and DVD+RW).
Rationale for selection	ISO/IEC 13346:1995 is a mature standard with broad industry support.
Maturity	Mature. Published as an ISO standard in 1995.
Forward outlook	Will remain popular.
Version and rationale for version	ISO/IEC 13346:1995 is the published ISO standard.
Limitations on the use of this standard	None

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.17 Animation

Justification for inclusion and usage

Defines the applications and formats to be used for the interchange of animated content between bureaux and departments and third parties.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Macromedia Flash	Macromedia Flash (.swf)	None
Apple QuickTime	Apple QuickTime (.qt, .mov, .avi)	
Macromedia Shockwave	Macromedia Shockwave (.swf)	
Remarks:		
The content provider should ensure that appropriate viewers/codecs are openly accessible to the consumer (e.g. as freeware downloadable from the Internet), and should provide a pointer to the viewer/codecs as necessary.		

Recommended standards

Standard 1 Macromedia Flash (.swf)	
Description	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 an antialiased, resizable file format that is small enough to stream across a normal modem connection.
Rationale for selection	Very commonly used format for animation on the Web, with freely available players and browser plug-ins.
Maturity	Mature.
Forward outlook	Will continue to be a commonly used format.
Version and rationale for version	A specific version need not be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitations on the use of this standard	Content providers should ensure that standard codecs appropriate to the content format are used, or that consumers are provided with links to download appropriate codecs for the viewers in question. As a general practice, the content provider should provide the consumer with a link to download the viewer best for rendering the content
Standard 2 Apple QuickTime (.qt, .mov, .avi)	
Description	QuickTime is a multimedia development, storage, and playback technology from Apple. QuickTime files combine sound, text, animation, and video in a single file. Apart from local playback, it can also support delivering streamed video/audio to consumers over network.

Standard 2 Apple QuickTime (.qt, .mov, .avi)	
Rationale for selection	Commonly used format for animation on the Web, with freely available players and browser plug-ins.
Maturity	Mature.
Forward outlook	Will continue to be a commonly used format
Version and rationale for version	A specific version need not be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitations on the use of this standard	Content providers should ensure that standard codecs appropriate to the content format are used, or that consumers are provided with links to download appropriate codecs for the viewers in question. As a general practice, the content provider should provide the consumer with a link to download the viewer best for rendering the content

Standard 3 Macromedia Shockwave (.swf)	
Description	The Shockwave Player displays Web content that has been created by Macromedia Director Shockwave Studio.
Rationale for selection	Commonly used format for animation on the Web, with freely available players.
Maturity	Mature.
Forward outlook	Will continue to be a commonly used format.
Version and rationale for version	A specific version need not be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitations on the use of this standard	Content providers should ensure that standard codecs appropriate to the content format are used, or that consumers are provided with links to download appropriate codecs for the viewers in question. As a general practice, the content provider should provide the consumer with a link to download the viewer best for rendering the content

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.18 Moving image and audio/visual

Justification for inclusion and usage

Defines a compressed format to be used for the interchange of audio/visual content such as movies.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
MPEG-1 (ISO 11172) .mp3 (ISO 11172) MPEG-2 MPEG-4 (ISO 14496) .wav .mid	MPEG-1 (ISO 11172) – for video and audio .mp3 (ISO 11172) – for audio MPEG-4 (ISO 14496) – for video and audio	None
<p>Remarks:</p> <p>The content provider should ensure that appropriate viewers/codecs are openly accessible to the consumer (e.g. as freeware downloadable from the Internet), and should provide a pointer to the viewer/codecs as necessary.</p>		

Recommended standards

Standard 1 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.
Rationale for selection	International ISO Standard (11172) for compression, decompression, processing and coded representation of moving pictures, audio and their combination. MPEG players are freely available.
Maturity	MPEG-1 approved in 1992.
Forward outlook	MPEG-1 will remain the dominant standard for audio and video on the Internet. Development of MPEG-4 will continue with development of additional standards, including MPEG-21 (a multimedia framework).
Version and rationale for version	MPEG-1. Version standardised by ISO.
Limitations on the use of this standard	None.

Standard 2 .mp3	
Description	MP3 (MPEG-1 Audio Layer-3) is a standard technology and format for compression of a sound while preserving the original level of sound quality when it is played.
Rationale for selection	International ISO Standard (11172) for compression, decompression, processing and coded representation of moving pictures, audio and their combination. MP3 players are freely available.
Maturity	MPEG-1 approved in 1992.
Forward outlook	MP3 will remain a dominant standard for audio on the Internet. Development of MPEG-4 will continue with development of additional standards, including MPEG-21 (a multimedia framework).

Standard 2 .mp3	
Version and rationale for version	MP3 (MPEG-1 Audio Layer-3). Version standardised by ISO.
Limitations on the use of this standard	None.

Standard 3 MPEG-4 (ISO 14496)	
Description	<p>MPEG-4 is an ISO/IEC standard developed by MPEG (Moving Picture Experts Group). MPEG-4 is the result of an international effort involving hundreds of researchers and engineers from all over the world. MPEG-4, with its ISO/IEC designation 'ISO/IEC 14496', was finalised in October 1998 and became an International Standard in the first months of 1999. The fully backward compatible extensions under the title of MPEG-4 Version 2 were frozen at the end of 1999, to acquire the formal International Standard Status early in 2000.</p> <p>Several extensions were added since and work on some specific work-items is still in progress. MPEG-4 builds on the proven success of three fields:</p> <ul style="list-style-type: none"> • Digital television; • Interactive graphics applications (synthetic content); • Interactive multimedia (World Wide Web, distribution of and access to content) <p>Currently, MPEG-4 is still developing and is divided into 23 parts.</p> <p>H.264, a high compression digital video compression standard that has become popular recently, was developed under the partnership effort from the ITU-T and the ISO/IEC (International Electrotechnical Commission). ITU-T's H.264 standard is technically equivalent to ISO/IEC's MPEG-4 AVC standard (the standard specified in MPEG-4 Part 10). Therefore, H.264 is often referred to as "H.264/MPEG-4 AVC".</p>
Rationale for selection	MPEG-4 provides the standardised technological elements enabling the integration of the production, distribution and content access with good compression capability. There are a number of MPEG-4 players available, some of which are free to use.
Maturity	MPEG-4 was approved in 1998.
Forward outlook	Growing adoption in production and distribution of multimedia contents is anticipated.
Version and rationale for version	MPEG-4. Version standardised by ISO.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
MPEG-2	<p>MPEG-2 extends the basic MPEG system to provide compression support for TV quality transmission of digital video.</p> <p>MPEG-2 is focused on the digital TV environment. It is therefore not felt to be appropriate for consideration as a candidate or emerging standard for Moving Image and Audio/Visual in the context of the IF. MPEG-4 is included as an emerging standard for future consideration. In determining the candidate standards it is considered that, in the context of the IF, MPEG-1 and MPEG-4 are sufficient, with MPEG-1 being the recommended standard.</p>
.wav	<p>WAVE (.wav) format is a Microsoft standard file format, based on Resource Interchange File Format (RIFF), for the storage of waveform audio data.</p> <p>Although .wav is a <i>de facto</i> standard for audio on Windows-based PCs, it is not recommended because, unlike MPEG-1 and mp3, it is not an open standard</p>
.mid	<p>MIDI (Musical Instrument Digital Interface) is a protocol designed for recording and playing back music on digital synthesizers that is supported by many makes of personal computer sound cards. Rather than representing musical sound directly, it transmits information about how music is produced.</p> <p>MIDI is not recommended on the basis that sound quality is dependent on the capabilities of sound card synthesizers and MPEG-1 and mp3 are the dominant standards for audio on the Internet.</p>

3.2.1.19 Audio/video streaming

Justification for inclusion and usage

Defines the formats to be used for the interchange of streaming audio/visual content e.g. Web casts between bureaux and departments and third parties.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
RealAudio / RealVideo Windows Media Formats Apple QuickTime MPEG-4	RealAudio / RealVideo (.ra, .ram, .rm, .rmm) Windows Media Formats (.asf, .wma, .wmv)	MPEG-4 (ISO 14496)
<p>Remarks:</p> <p>The content provider should ensure that appropriate viewers/codecs are openly accessible to the consumer (e.g. as freeware downloadable from the Internet), and should provide a pointer to the viewer/codecs as necessary.</p>		

Recommended standards

Standard 1 RealAudio/RealVideo (.ra, .ram, .rm, .rmm)	
Description	Proprietary format from Real Networks for receiving streamed content in real time.

Standard 1 RealAudio/RealVideo (.ra, .ram, .rm, .rmm)	
Rationale for selection	One of the most commonly used formats for continuous streaming of audio and video with browser plug-ins and players freely available.
Maturity	Mature.
Forward outlook	Will continue to be a commonly used format.
Version and rationale for version	A specific version need not be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitations on the use of this standard	Content providers should ensure that standard codecs appropriate to the content format are used, or that consumers are provided with links to download appropriate codecs for the viewers in question. As a general practice, the content provider should provide the consumer with a link to download the viewer best for rendering the content

Standard 2 Windows Media Formats (.asf, .wma, .wmv)	
Description	Proprietary format from Microsoft for receiving streamed content in real time.
Rationale for selection	Commonly used format for audio/video streaming on the Web, with freely available players.
Maturity	Mature.
Forward outlook	Will continue to be a commonly used format.
Version and rationale for version	A specific version need not be specified, on the basis that members of the public have access to free software for processing these types of files.
Limitations on the use of this standard	Content providers should ensure that standard codecs appropriate to the content format are used, or that consumers are provided with links to download appropriate codecs for the viewers in question. As a general practice, the content provider should provide the consumer with a link to download the viewer best for rendering the content

Emerging standards for future consideration

Emerging Standard(s)	Description
MPEG-4 (ISO 14496)	Please refer to the area on “Moving image and audio/visual” for details on MPEG-4 (ISO 14496)

Other Candidate Standards

Other Standard(s)	Description
Apple QuickTime	Please refer to the area on “Animation” for details on Apple QuickTime

3.2.1.20 E-business document / data message formatting language

Justification for inclusion and usage

Language to be used to define the format of data messages and e-business documents (e.g. invoices and purchase orders).

Relevant to submissions under ETO : Business specific XML schemas will be published where relevant.

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
XML	XML and related W3C recommendations produced by the W3C XML Core Working Group	None
Remarks: XML users are recommended to create or generate XML 1.0 documents if they do not need the new features in XML 1.1, and to ensure as far as possible that their XML parsers can understand both XML 1.0 and XML 1.1.		

Recommended standards

Standard 1 XML and related W3C recommendations produced by the W3C XML Core Working Group	
Description	XML defines a universal format for structured documents and data.
Rationale for selection	XML is a W3C standard. XML is supported by a broad range of application development, software infrastructure, business applications and industry-specific schema initiatives.
Maturity	XML 1.0 was approved as a W3C recommendation in February 1998. XML 1.1 was approved as a W3C recommendation in February 2004.
Forward outlook	W3C XML Core Working Group will continue to update XML and related W3C specifications.
Version and rationale for version	Users should follow the W3C XML Core Working Group's recommendations, including recommendations on the choice between different versions of XML standard.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.21 XML schema definition

Justification for inclusion and usage

Provides a language for defining schemas for XML messages/documents.

Relevant to submissions under ETO : Business specific XML schemas will be published where relevant.

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
XML Schema Document Type Definition (DTD) Relax NG	XML Schema 1.0 – for data-oriented message exchange and processing DTD as defined in the corresponding XML specification – for textual document-oriented applications	Relax NG

Recommended standards

Standard 1 XML Schema 1.0	
Description	XML Schema defines the structure and content of XML documents.
Rationale for selection	XML Schema is a W3C standard. XML Schema is appropriate for data-oriented message exchange and processing.
Maturity	XML Schema was approved as a W3C Recommendation on 2 May 2001.
Forward outlook	The W3C is currently working to develop a set of requirements for XML Schema 1.1.
Version and rationale for version	Version 1.0. Current specification.
Limitations on the use of this standard	None.

Standard 2 Document Type Definition (DTD) as defined in the corresponding XML specification	
Description	Document Type Definition (DTD) is a specific definition that follows the rules of the Standard Generalized Markup Language (SGML). A DTD is a specification that accompanies a document and identifies what the markup is that separates paragraphs, identifies topic headings, and so forth and how each is to be processed. In XML, a DTD is used for declaring constraints on the use of this markup.
Rationale for selection	DTD is still commonly used for textual document-oriented applications and is widely supported by tools such as content management systems and structured editors.
Maturity	DTD is defined as part of the XML standard. XML 1.0 was approved as a W3C recommendation in February 1998. XML 1.1 was approved as a W3C recommendation in February 2004.
Forward outlook	W3C XML Core Working Group will continue to update XML and related W3C specifications.
Version and rationale for version	As DTD is part of the XML standard, the version of DTD to use should follow the user's choice on the version of XML.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
RELAX NG	RELAX NG is developed by the Relax NG Technical Committee of OASIS based on REgular LAnguage description for XML RELAX – for describing XML-based

	languages – and Tree Regular Expressions for XML (TREC) and is designed to be a simple and easy to use alternative to XML Schema. Version 1.0 of the specification was published in December 2001. It was published as ISO standard (ISO/IEC 19757-2:2003) in December 2003.
--	--

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.22 XML message encryption

Justification for inclusion and usage

Required to encrypt/decrypt digital content (including XML documents and portions thereof) and to define a syntax to represent the (1) encrypted content and (2) information that enables an intended recipient to decrypt it.

Relevant to submissions under ETO : To be specified along with the business specific XML schema.

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
XML Encryption	XML Encryption	None

Recommended standards

Standard 1 XML Encryption	
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. The relevant specifications include : - XML Encryption Syntax and Processing - Decryption Transform for XML Signature
Rationale for selection	XML Encryption is a W3C recommendation, and is the only available standard for XML message encryption.
Maturity	XML Encryption has become a W3C Recommendation on 10 December 2002.
Forward outlook	The XML Encryption working group has announced that it has successfully advanced all chartered deliverables to their final state and the charter has expired; presently the mailing list may be used to ask questions about the specifications or interop report.
Version and rationale for version	Currently, only one version of XML Encryption exists.
Limitations on the use of this standard	None

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.23 XML message signing

Justification for inclusion and usage

Required for digital signing of XML.

Relevant to submissions under ETO : To be specified along with the business specific XML schema.

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
XML Signature	XML Signature	None

Recommended standards

Standard 1 XML Signature	
Description	XML Signatures provide <i>integrity, message authentication, and/or signer authentication</i> services for data of any type. In this context, our concern is limited to the digital signing of XML documents / messages. The specifications relevant to our concern include : - XML-Signature Syntax and Processing .
Rationale for selection	XML Signature is a joint W3C/IETF standard, and the only one available for XML message signing.
Maturity	XML-Signature Requirements specification completed W3C Last Call in August 1999 and has been published as Informational RFC 2807. In February 2002 the XML Signature Syntax and Processing specification was published as a W3C Recommendation and then was published as an IETF Standard RFC 3275.
Forward outlook	The XML Signature working group has announced that it has successfully advanced all chartered deliverables to their final state and the charter has expired; presently the mailing list may be used to ask questions about the specifications or interop report.
Version and rationale for version	Currently, only one version of XML Signature exists.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.1.24 Content syndication

Justification for inclusion and usage

Formats of content delivery and syndication by web portals.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
RSS	RDF Site Summary (RSS) 1.0	Atom
Atom	Really Simple Syndication (RSS) 2.0	
Remarks:		
The content provider is free to use either RSS 1.0 or 2.0, while the content consumer should ensure that the RSS Reader can support both RSS 1.0 and 2.0.		

Recommended standards

Standard 1 RSS	
Description	RSS is an XML-based format for distributing and aggregating Web content. It was originated by Netscape in the late 90s (version 0.90) as a format for building headline portals for mainstream news sites. Subsequently, with version 0.90 as the basis, UserLand Software proposed a simpler version 0.91 and developed today's version 2.0. In parallel with this, the RSS-DEV working group, a third party non-commercial group, was engaged in a separate stream of development to design another format based on version 0.90, namely RSS 1.0. Although they share the same name, RSS 1.0 and 2.0 are two different and competing specifications. The major difference is that RSS 1.0 is based on RDF while RSS 2.0 is not.
Rationale for selection	Both RSS 1.0 and 2.0 are widely used in RSS-ready Web sites/portals. Most of the common RSS Readers provide support for both formats.
Maturity	Netscape released the first version of RSS, version 0.90, in March 1999. Version 1.0 (by RSS-DEV working group) and version 2.0 (by UserLand) were released in December 2000 and September 2002 respectively.
Forward outlook	The number of Web sites/portals adopting RSS is increasing. Besides the availability of free RSS Readers and plug-ins, support of RSS is natively included in the latest/next versions of the common browsers (include Mozilla Firefox, Microsoft Internet Explorer, etc).
Version and rationale for version	RSS 1.0 and 2.0 are two different specifications and both are mature and actively used. Most RSS tools support both versions.

Standard 1 RSS	
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
Atom	Because of the confusion of the different versions of RSS and the perceived deficiencies in both RSS 1.0 and 2.0, a third group started a new syndication specification, Atom, in June 2003. The work was later adopted by Internet Engineering Task Force (IETF). The Atom Syndication Format was approved as an IETF Proposed Standard in August 2005. However, its wide adoption in the industry is yet to be noted when compared to RSS.

Other Candidate Standards

Other Standard(s)	Description
None	

3.2.2 Interoperability areas for future consideration – no apparent need yet**3.2.2.1 Vector graphics (non GIS/mapping application)****Justification for inclusion and usage**

Defines the format to be used to enable the interchange of vector graphics. 2 and 3 dimensional graphical file types such as JPEG and GIF (raster graphics) contain information that is directly mapped to the display e.g. a screen or a printer. Vector graphics, in contrast, consist of commands or statements that describe how lines and shapes are represented and are therefore smaller and easier to manipulate. Vector graphics are typically converted into raster graphics images prior to display.

Vector graphics are commonly used by animation products and also by products from companies such as Adobe. When used in such products, the graphics are typically rendered through raster formats such as JPEG and GIF.

The industry trend is to use graphics tools to generate vector graphics and then let the browser handle the rendering. In the future, Government may wish to utilise tools which generate vector graphics to provide for more efficient and flexible delivery of graphical content.

Standards for future consideration

Standard(s)	Description
Scalable Vector Graphics	<p>SVG is a W3C recommended standard for describing two-dimensional graphics in XML. SVG allows for three types of graphic objects: vector graphic shapes (e.g. paths consisting of straight lines and curves), images and text. Graphical objects can be grouped, styled, transformed and composited into previously rendered objects. The feature set includes nested transformations, clipping paths, alpha masks, filter effects and template objects.</p> <p>SVG drawings can be interactive and dynamic. Animations can be defined and triggered either declaratively (i.e., by embedding SVG animation elements in SVG content) or via scripting.</p> <p>SVG is suitable for display on small devices (SVG Mobile Profiles).</p> <p>SVG v1.0 was approved as a W3C Recommendation in September 2001 and SVG v1.1 was approved as a W3C Recommendation in January 2003.</p> <p>The W3C is working on development of SVG v1.2</p>

3.2.2.2 Content/data resource description language

Justification for inclusion and usage

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 describing documents to ensure consistent understanding and terminology. This standard enables 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. E-GMS has adopted the Dublin Core for the attributes (metadata) and has extended based on it. Australia and New Zealand have implemented their Government Locator Services which are based on well described content. If the HKSARG is looking for a better way to manage its web content / data resource, it may consider adopting a similar approach.

Standards for future consideration

Standard(s)	Description
Resource Description Framework	<p>The Resource Description Framework (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 mechanisms for declaring these properties, nor does it provide any mechanisms for defining the relationships between these properties and other resources. That is the role of RDF Schema.</p> <p>The RDF suite of specifications consists of a number of components:</p>

Standard(s)	Description
	<ul style="list-style-type: none"> • RDF/XML Syntax Specification • Resource Description Framework (RDF): Concepts and Abstract Syntax • RDF Vocabulary Description Language 1.0: RDF Schema • RDF Primer • RDF Semantics • RDF Test Cases <p>The Resource Description Framework 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.</p> <p>RDF Model and Syntax Specification was approved as a W3C Recommendation in September 2001. The RDF suite was approved as a W3C Recommendation in February 2004.</p> <p>In March 2004, the W3C Membership approved two new Working Groups, “Best Practices and Deployment” and “RDF Data Access”, to facilitate this development and ease the sharing of data located across distributed collections.</p>

3.2.3 Interoperability areas for future consideration –standards not matured yet

3.2.3.1 Inter-organisation radio frequency identification

Justification for inclusion and usage

Required to facilitate the transmission, encoding and sharing of item information stored in radio frequency identification (RFID) tags by different application across organisations.

Standards for future consideration

Standard(s)	Description
<p>The suite of RFID related specifications from EPCglobal</p> <p><i>(see the specific standards listed below in this table)</i></p>	<p>This suite of specifications is designed for applying to supply chain management. It provides the overall system definition and how functional requirements are partitioned across various subsystems.</p> <p>The Electronic Product Code (EPC) is a unique number that identifies a specific item in the supply chain. EPC is promoted by EPCglobal.</p> <p>EPCglobal is a joint venture between GS1 and the GS1 US. Due to GS1 and GS1 US’s history in developing the Universal Product Code (UPC), which is applied to the barcode system of major supply chains, EPC will be adopted by many major suppliers and technology providers. In the early development of various RFID projects around the world, EPC has been adopted by major suppliers and technology providers.</p> <p>The International Standards Organization (ISO) has approved the EPC Gen2 Class 1 UHF standard to its 18000-6C standard. The implementation of RFID solutions with the full suite of specifications may not be necessary in some cases. We shall consider further categorization of interoperability areas in the next review exercise. At present, the suite comprises the following specifications :</p>

Standard(s)	Description
EPC Tag Data Specification Version 1.1 Rev. 1.27	<p>The EPC Tag Data Specification provides a standard way in which the item information, such as product ID, is stored on an RFID tag. It ensures interoperability as different applications will use the same set of data encoding scheme.</p> <p>The EPC Tag Data Specification encompasses the specific encoding schemes for a serialized version of the EAN.UCC Global Trade Item Number (GTIN®), the EAN.UCC Serial Shipping Container Code (SSCC®), the EAN.UCC Global Location Number (GLN®), the EAN.UCC Global Returnable Asset Identifier (GRAI®), the EAN.UCC Global Individual Asset Identifier (GIAI®), and a General Identifier (GID).</p>
900 MHz Class 0 Radio Frequency Identification Tag Specification	It specifies the communication interface and protocol for 900 MHz Class 0 RFID Tag operation (i.e. write once read many). It includes the RF and tag requirements and provides operational algorithms to enable communication in this band.
13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification	This specification defines the communication interface and protocol for 13.56 MHz Class 1 RFID Tag operation. It also includes the RF and tag requirements to enable communication in this band.
Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9	It specifies the radio frequency communication interface and Reader commanded functionality requirements for Class I RFID Tag operating in the frequency range of 860MHz–960MHz. A Class I tag is designed to communicate only its unique identifier and other information required to obtain the unique identifier during the communication process. OFTA approved a dual-band frequency (865-868MHz and 920-925MHz) for UHF RFID application in HK.
Reader Protocol	This specification defines the communication messaging and protocol between tag readers and EPC compliant software applications.
Application Level Event (ALE) Specification Version 1.0	This EPCglobal Board-ratified standard specifies an interface through which clients may obtain filtered, consolidated Electronic Product Code™ (EPC) data from a variety of sources.
Physical Markup Language (PML) Core Specification	The Physical Markup Language (PML) is a collection of common, standardized XML vocabularies to represent and distribute information related to EPC Network enabled objects. The PML standardizes the content of messages exchanged within the EPC network. It is, therefore, part of the Auto-ID Center’s effort to develop standardized interfaces and protocols for the communication with and within the Auto-ID infrastructure. The core part of the physical mark-up-language (PML Core) provides a standardized format for the exchange of the data captured by the sensors in the Auto-ID infrastructure, e.g. RFID readers. The Auto-ID PML Core specification 1.0 defines the syntax and semantics of PML Core. This specification also includes XML Schema and Instance files for reference.

Standard(s)	Description
Object Naming Service (ONS) Specification Version 1.0	The ONS provides a global lookup service to translate an EPC into one or more Internet Uniform Reference Locators (URLs) where further information on the object may be found. These URLs often identify an EPC Information Service, though ONS may also be used to associate EPCs with web sites and other Internet resources relevant to an object. ONS provides both static and dynamic services. Static ONS typically provides URLs for information maintained by an object's manufacturer. Dynamic ONS services record a sequence of custodians as an object moves through a supply chain. ONS is built using the same technology as DNS, the Domain Name Service of the Internet. This document defines the working of ONS and its interface to applications.
EPCglobal Architecture Framework Version 1.0	This document defines and describes the EPCglobal Architecture Framework. The EPCglobal Architecture Framework is a collection of interrelated standards for hardware, software, and data interfaces, together with core services that are operated by EPCglobal and its delegates, all in service of a common goal of enhancing the supply chain through the use of Electronic Product Codes™ (EPCs).

3.2.3.2 Electronic form

Justification for inclusion and usage

Defines the next generation of forms for the Web.

Remarks:

Project teams that deploy electronic form (e-form) for data collection should evaluate the features and costs of the e-form products according to their project requirements and choose a suitable e-form product on the condition that the target form users can easily use the e-form, e.g. software or plug-in for rendering the form are freely downloadable and are executable on common client configurations.

Standards for future consideration

Standard(s)	Description
XForms	By splitting traditional XHTML forms into three parts—XForms model, instance data, and user interface—it separates presentation from content, allows reuse, gives strong typing—reducing the number of round-trips to the server, as well as offering device independence and a reduced need for scripting. XForms is not a free-standing document type, but is intended to be integrated into other markup languages, such as XHTML. Version 1.1 has been published as a Working Group Note for comments. On 29 October 2007, XForms 1.0 Third Edition was published as a W3C Recommendation, which adds clarifications and corrects errors as reported in the previous edition errata. On 29 November 2007, XForms 1.1 was published as a W3C Candidate Recommendation.

3.3 SECURITY DOMAIN

3.3.1 Interoperability areas for immediate consideration

3.3.1.1 IP network-level security

Justification for inclusion and usage

Required to provide network level security. The IP network level security standards can be used for implementing virtual private networks (VPNs) and secure remote

access, with the advantage that it does not require changes to the client and server computers, as it is implemented at the network level. IP network level security also provides for authentication of the originating computer.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
IPsec	IPsec	None

Recommended standards

Standard 1 Internet Protocol Security (IPsec)	
Description	IPsec (Internet Protocol Security) is a standard for security at the network or packet processing layer of network communication.
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.
Maturity	In December 2005, a third generation documents RFCs 4301–4309 were published which are largely a superset of the earlier standards (RFC 2401–2412) introduced in 2001. The latest Windows 2003 Server also has built in support of IPsec.
Forward outlook	IPsec will remain the dominant standard. It should be noted that IPv6 is required to support the full implementation of IPsec.
Version and rationale for version	Not applicable – there is only one version available at present.
Limitations on the use of this standard	While there is little debate about whether IPsec is the right choice for IP security, this does not mean there are no challenges in its implementation. The biggest challenge with IPsec is managing VPN membership and the associated distribution of keys. This administration is labour intensive, and demands skills and experience that are in short supply. The e-security industry is now rolling out IPsec management tools that provide a simple point-and-click interface to simplify IPsec provisioning and administration. As these tools prove themselves and gain adoption, this challenge will be greatly reduced. However, while these tools will greatly reduce the administration, the lack of expertise in designing security policies will remain a barrier to further IPsec adoption. 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 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.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.2 Transport-level security

Justification for inclusion and usage

Required to support transport level security. Transport-level security enables authentication of clients and servers and encryption of data when using TCP/IP-based protocols such as HTTP.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
SSL	SSL v3.0	None
TLS	TLS v1.0	
Remarks:		
New implementations should ready themselves to support TLS and should ensure their TLS implementation's backward compatibility with SSL v3 where situation allows.		

Recommended standards

Standard 1 Secure Sockets Layer (SSL) v3.0	
Description	The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
Rationale for selection	SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the <i>de facto</i> standard until evolving into Transport Layer Security (TLS). Although TLS has been proposed by the IETF as the successor to SSL, it is likely that SSL will remain in widespread use for a considerable period.
Maturity	Mature. Netscape final draft specification, November 1996. The IETF TLS Working Group began working with SSL v3.0 in 1996.
Forward outlook	Although SSL is likely to remain in use for a considerable period, TLS has been proposed as its successor and is in the early stages of adoption.
Version and rationale for version	SSL v3.0 is the latest version of SSL.

Standard 1 Secure Sockets Layer (SSL) v3.0	
Limitations on the use of this standard	None. SSL is available in most browsers with either 40 bit or 128-bit encryption. There are now no restrictions on using 128 bit.

Standard 2 Transport Layer Security (TLS) v1.0	
Description	<p>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, allowing the two to coexist.</p> <p>The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications.</p> <p>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).</p>
Rationale for selection	<p>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 significant community review, and appears to enjoy enough community interest to be considered valuable.</p> <p>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, allowing the two to coexist. Thus, provided that implementations conform to the standards it should be possible for an SSL v3.0 application to communicate with a TLS v1.0 application.</p> <p>TLS is virtually universally available, through support within browsers and web servers.</p>
Maturity	<p>TLS v1.0 is outlined in the IETF's RFC 2246 dated January 1999.</p> <p>IETF updated RFC 2246 by RFC 3546 dated June 2003 which describes both generic extension mechanisms for the TLS handshake client and server hellos, and specific extensions using these generic mechanisms. The extensions are backwards compatible – communication is possible between TLS v1.0 clients that support the extensions and TLS v1.0 servers that do not support the extensions, and vice versa.</p> <p>The latest version, TLS v1.1, was published as RFC 4346 in April 2006 which clarifies some ambiguities and adds a number of recommendations.</p>
Forward outlook	The TLS Working Group, established in 1996, continues to work on the TLS protocol and related applications.
Version and rationale for version	TLS v1.0 is recommended as v1.1 has just been announced and it may take some time before industry adoption.
Limitations on the use of this standard	Early versions of web server software exhibited interoperability problems between TLS v1.0 and SSL v3.0. Confirmation should be sought 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.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.3 Symmetric encryption algorithms

Justification for inclusion and usage

Encryption algorithms are used to ensure confidentiality of information. Symmetric encryption algorithms are required to enable the exchange of large volumes of encrypted data.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
DES 3DES AES Blowfish IDEA RC4	DES 3DES – comparatively harder to break AES – comparatively harder to break	None
<p>Remarks:</p> <p>The choice of algorithms depends on the level of security required. In addition, AES supports key lengths of 128, 192 and 256 bits offering different levels of cryptographic strengths. The interacting parties should either agree before implementation on the algorithm to use or should enable some auto-negotiation mechanism.</p>		

Recommended standards

Standard 1 Data Encryption Standard (DES)	
Description	Data Encryption Standard (DES) has been a widely-used method of data encryption using a private (secret) key. There are 72×10^{15} possible encryption keys that can be used. For each given message, the key is chosen at random. Both the sender and the receiver must know and use the same private key. DES supports a key length of 56 bits.
Rationale for selection	DES was specified in the ANSI X3.92 and X3.106 standards and in the Federal FIPS 46 and 81 standards. It has been very widely used and highly mature.
Maturity	DES originated at IBM in 1977 and was adopted by the U.S. Department of Defense.
Forward outlook	Given the relatively low strength of DES as compared with newer encryption algorithms and the rapid increase of computing power that can be used for brute-forcing, NIST has encouraged Federal government organisations to use AES for some time. The trend is that DES will eventually be superseded by AES.

Standard 1 Data Encryption Standard (DES)	
Version and rationale for version	Not applicable – there is only one version.
Limitations on the use of this standard	NIST withdrew FIPS 46-3 on 19 May 2005. DES should be used only for environments that require lower level of security.

Standard 2 Triple DES (3DES)	
Description	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. 3DES supports a key length of 168 bits.
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.
Maturity	Based on a standard developed in 1977.
Forward outlook	Likely to be eventually superseded by AES.
Version and rationale for version	Not applicable – there is only one single version.
Limitations on the use of this standard	None.

Standard 3 Advanced Encryption Standard (AES)	
Description	The Advanced Encryption Standard (AES) is a symmetric block cipher algorithm that can encrypt (encipher) and decrypt (decipher) information. It is based on the Rijndael algorithm, named after the Belgian researchers Vincent Rijmen and Joan Daemen, who developed it. It has been announced as FIPS-197 standard for the US Government agencies and, as a likely consequence, is becoming the de facto encryption standard for commercial transactions in the private sector. AES supports key lengths of 128, 192 and 256 bits.
Rationale for selection	AES supports key sizes of 128 bits, 192 bits and 256 bits and will serve as a replacement for the Data Encryption Standard (DES), which has a key size of 56 bits. In addition to the increased security that comes with larger key sizes, AES can encrypt data much faster than 3DES.
Maturity	In September 1997, NIST issued a Federal Register notice soliciting an unclassified, publicly disclosed encryption algorithm that would be available royalty-free worldwide. NIST studied all available information and analysis about the candidate algorithms, and selected one of the algorithms, the Rijndael algorithm, to be adopted as the AES. AES was announced and published as FIPS-197 on November 26, 2001 and became effective on May 26, 2002.
Forward outlook	AES, already a standard for new implementations in the US government, is gradually being rolled out in many different encryption protocols including IEEE 802.11, IPsec (Internet Draft), S/MIME (RFC3565), and TLS (RFC 3268).

Standard 3 Advanced Encryption Standard (AES)	
Version and rationale for version	Not applicable – there is only one single version.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
IDEA	Not considered as it is patented and requires a licence for all but personal use. IDEA supports a key length of 128 bits.
Blowfish	Not recommended as it is not adopted widely by commercial products and is not included in higher-level security standards such as SSL/TLS, IPsec, S/MIME or PKCS. Blowfish supports key lengths of 32-448 bits.
RC4	RC4 is a stream cipher designed by Rivest for RSA Security. It is a variable key-size stream cipher. RC4 is used for file encryption in products such as RSA SecurPC. It is also used for secure communications, as in the encryption of traffic to and from secure web sites using the SSL protocol. Stream ciphers, such as RC4, were considered for the IF. However, they have not been recommended for standalone use because, unless they are implemented correctly, they can be prone to cryptographic weakness. This contrasts with their use in higher-level specifications, such as SSL, which are implemented by professional development organisations and have been rigorously tested in the field.

3.3.1.4 Asymmetric encryption algorithms

Justification for inclusion and usage

Encryption algorithms are used to ensure confidentiality of information. Asymmetric encryption algorithms enable the sender to encrypt data using the recipient’s public key.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
RSA ECC	RSA	Elliptic Curve Cryptography (ECC) (RFC 3278)

Recommended standards

Standard 1 RSA	
Description	<p>RSA is a proprietary public-key cryptography system, from 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. The benefit of this approach, in comparison to symmetric encryption, is that different (but related) keys are used for encryption and decryption, so the encryption key can be freely published. The downside is that the asymmetric keys must be longer than symmetric keys to offer the same level of security and so are computationally more intensive.</p> <p>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.</p>
Rationale for selection	<p>RSA is the dominant asymmetric encryption scheme. The ISO (International Standards Organisation) 9796 standard lists RSA as a compatible cryptographic algorithm.</p>
Maturity	<p>The RSA system was first developed in 1997 and is thus mature and has been extensively tested.</p>
Forward outlook	<p>RSA is the dominant asymmetric encryption algorithm and will continue to be developed by RSA Security.</p>
Version and rationale for version	<p>Only one version of RSA exists.</p>
Limitations on the use of this standard	<p>The use of RSA for encryption is significantly slower than symmetric encryption algorithms. The longer keys required are such that it utilises significantly more computational resource. RSA states that DES is at least 100 times faster in software and 1,000 to 10,000 times faster in hardware. It is thus not appropriate for large data volumes.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
<p>Elliptic curve cryptography (ECC) (RFC 3278)</p>	<p>Elliptic curve cryptography has emerged as a promising new branch of public-key cryptography in recent years, due to its potential for offering similar security to established public-key cryptosystems at reduced key sizes. Improvements in various aspects of implementation, including the generation of elliptic curves, have made elliptic curve cryptography more practical than it was when first introduced in the 1980s.</p> <p>The use of ECC in Cryptographic Message Syntax is in the Informational RFC 3278 published in April 2002.</p> <p>If ECC is used over a prime field then the elliptic curve size should be at least 192 bits and if over a binary field then the elliptic curve size should be at least 163 bits.</p> <p>To provide the equivalent level of security to 3DES over a prime field then the elliptic curve size should be 224 bits and over a binary field 233 bits.</p> <p>To provide the equivalent level of security to AES (128-bit) over a prime field then the elliptic curve size should be 256 bits and over a binary field 283 bits.</p> <p>To provide the equivalent level of security to AES (192-bit) over a prime field then the elliptic curve size should be 384 bits and over a binary field 409 bits.</p> <p>To provide the equivalent level of security to AES (256-bit) over a prime field then the elliptic curve size should be 521 bits and over a binary field 571 bits.</p>

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.5 Digital signature algorithms

Justification for inclusion and usage

Required for the generation and verification of digital signature in use with public key infrastructure (PKI) to provide authentication, integrity, and non-repudiation functions.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
DSA RSA for Digital Signatures ECDSA	DSA RSA for Digital Signatures	ECDSA
<p>Remarks:</p> <p>The interacting parties should either agree before implementation on the algorithm to use or should enable some auto-negotiation mechanism.</p>		

Recommended standards

Standard 1 DSA (Digital Signature Algorithm)	
Description	<p>The National Institute of Standards and Technology (NIST) published the Digital Signature Algorithm (DSA) in the Digital Signature Standard (DSS), which is 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.</p> <p>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.</p> <p>NIST defines key sizes of 512-1024 bits.</p>
Rationale for selection	<p>Together with RSA, DSA is an accepted standard for digital signature algorithms. It is the US Department of Commerce/NIST FIPS standard, specified in its Digital Signature Standard document FIPS 186.</p>
Maturity	<p>The Digital Signature Algorithm is a Federal Information Processing Standard (FIPS) issued on May 19,1994.</p>

Standard 1 DSA (Digital Signature Algorithm)	
Forward outlook	<p>Elliptic Curve Digital Signature Algorithm (ECDSA) specified in ANSI Standard X9.62 is the elliptic curve analogue of DSA. Efficiency and cryptographic strength will determine whether ECDSA supersedes DSA.</p> <p>The National Institute of Standards and Technology (NIST) is investigating the modification of DSA to accommodate larger key and message digest sizes, in order to make the algorithm's security commensurate with that of the future AES.</p>
Version and rationale for version	<p>Only one version of DSA exists. However, multiple examples of DSA are available. These examples use the 1024-bit modulus size. For examples, see http://csrc.nist.gov/groups/ST/toolkit/documents/dss/Examples-1024bit.pdf</p>
Limitations on the use of this standard	None.

Standard 2 RSA for Digital Signatures	
Description	<p>RSA for Digital Signatures is an alternative method for generating and checking digital signatures.</p> <p>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.</p>
Rationale for selection	RSA for Digital Signatures is recognised by the NIST within the Digital Signature Standard as an alternative to DSA or ECDSA.
Maturity	Proprietary standard introduced in February 2000, which has gained wide acceptance.
Forward outlook	RSA for Digital Signatures is likely to remain the widely supported standard for generating and checking digital signatures.
Version and rationale for version	Currently, there is only one version of RSA for Digital signatures.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
ECDSA	<p>The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). It was accepted in 1999 as an ANSI standard, and was accepted in 2000 as IEEE and NIST standards. It was also accepted in 1998 as an ISO standard, and is under consideration for inclusion in some other ISO standards.</p> <p>ECDSA is one of the three FIPS-approved algorithms for generating digital signatures, along with DSA and RSA. It has been accepted as an ANSI standard for financial services (ANSI X9.62).</p> <p>Although recognised as a standard by the US government, ECDSA is still considered an emerging standard for digital signature generation, and should be reviewed in the light of future support by PKI infrastructure providers. Verisign, the dominant provider, currently uses RSA for X.509 certificates.</p> <p>If ECDSA is used over a prime field then the elliptic curve size should be at least 192 bits and if over a binary field then the elliptic curve size should be at least 163 bits.</p>

	<p>To provide the equivalent level of security to 3DES over a prime field then the elliptic curve size should be 224 bits and over a binary field 233 bits.</p> <p>To provide the equivalent level of security to AES (128-bit) over a prime field then the elliptic curve size should be 256 bits and over a binary field 283 bits.</p> <p>To provide the equivalent level of security to AES (192-bit) over a prime field then the elliptic curve size should be 384 bits and over a binary field 409 bits.</p> <p>To provide the equivalent level of security to AES (256-bit) over a prime field then the elliptic curve size should be 521 bits and over a binary field 571 bits.</p>
--	--

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.6 Hashing algorithms for digital signature

Justification for inclusion and usage

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. The hashing algorithm is applied to the message to generate a message digest; the message digest is encrypted using a private key to create a digital signature. The receiver then applies the public key to the digital signature to decrypt the message digest; it applies the same hashing algorithm to the message to generate the message digest. If the two message digests match then the integrity of the received message has not been compromised.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
SHA-1 MD5 SHA-224, SHA-256, SHA-384 and SHA-512	SHA-1	SHA-224, SHA-256, SHA-384 and SHA-512

Recommended standards

Standard 1 SHA-1	
Description	SHA-1 converts the content of a message that is to be signed into a number that is incorporated into the signature which is placed on the document, before the signature is encrypted. This ensures that the encrypted signature which is sent with each message is different from that sent on other messages and cannot be re-used on a different message.

Standard 1 SHA-1	
Rationale for selection	The National Institute of Standards and Technology (NIST) has approved hash algorithm SHA-1 for digital signatures. SHA-1 is also described in ANSI X9.30 and ISO/IEC 10118-3:1998. SHA-1 is recommended above MD5 due to its larger message digest making it more secure against brute force collision and inversion attacks.
Maturity	Effective October 1995.
Forward outlook	In February 2005, NIST announced in a brief comment that it already planned to phase out SHA-1 in favour of the larger and stronger hash functions such as SHA-224, SHA-256, SHA-384 and SHA-512 by 2010.
Version and rationale for version	SHA-1 is defined in ANSI X9.30, National Institute of Standards and Technology (NIST), Announcement of Weakness in the Secure Hash Standard, 1994 and ISO/IEC 10118-3:1998. SHA-1 is the most widely adopted version among the different variations of SHA.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
SHA-224, SHA-256, SHA-384 and SHA-512	Stronger variants of the SHA-1 hash function with larger message digest size.

Other Candidate Standards

Other Standard(s)	Description
MD5	MD5 was developed by Professor Ronald L. Rivest in 1994. Its 128 bit (16 byte) message digest makes it a faster implementation than SHA-1. However, SHA-1 is suggested for use as brute force attack is harder (160 vs. 128 bits for MD5) (source Australian Defence Force). RFC 3110 states "By now there has been sufficient experience with SHA-1 that it is generally acknowledged to be stronger than MD5".

3.3.1.7 Cryptographic message syntax for file-based signing and encrypting

Justification for inclusion and usage

Provides a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes to enable the development of applications which support PKI, such as ESD. Standards for the syntax of cryptographic messages allow such applications to exchange cryptographic data.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
PKCS #7 RFC 3369	PKCS #7 v1.5 (RFC 2315)	RFC 3369

Recommended standards

Standard 1 PKCS #7 v1.5 (RFC 2315)
Please refer to the area “Attachment of digital signature to electronic documents received under ETO” for details on PKCS #7.

Emerging standards for future consideration

Emerging Standard(s)	Description
RFC 3369	Please refer to the area “Attachment of digital signature to electronic documents received under ETO” for details on RFC 3369.

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.8 On-line certificate status protocol

Justification for inclusion and usage

Enables the current status of a digital certificate to be determined without the use of a certificate revocation list. This protocol can be used by applications, typically for high-value or highly sensitive transactions, to perform an online checking of the status of a digital certificate, rather than relying on a periodic certificate revocation list (CRL).

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
RFC 2560	RFC 2560	None

Recommended standards

Standard 1 RFC 2560	
Description	Closely related to CRL checking. However, simple CRL checking is inefficient for ad-hoc enquiries. To check if a certificate is in a CRL, one must retrieve the whole CRL from the directory and then search through it. There is also often a lag between the time a certificate is revoked and the time that information is made known through the CRL. RFC 2560 specifies a protocol useful in determining the current status of a digital certificate without requiring CRLs.
Rationale for selection	RFC 2560 is an IETF standard, and the only viable one for on-line certificate status protocol.
Maturity	This standard is an IETF standard published in June 1999.
Forward outlook	The IETF Public-Key Infrastructure (pkix) working group will continue to track the evolution of these standards and incorporate changes and additions as appropriate.

Standard 1 RFC 2560	
Version and rationale for version	Only one version exists.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.9 Certification request

Justification for inclusion and usage

Defines the format of a request to a certification authority (CA) for a public-key certificate to enable the use of digital certificates issued by multiple certification authorities. This standard can be used to allow applications (e.g. payment, an e-commerce transaction, or a G2B interaction) to request certificates from multiple CAs using a common format.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
PKCS #10 CRMF	PKCS #10 v1.7 (RFC 2986)	Certificate Request Message Format (CRMF) (RFC 2511)

Recommended standards

Standard 1 PKCS #10 v1.7 (RFC 2986)	
Description	A certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. Certification requests are sent to a CA, which transforms the request into an X.509 public-key certificate.
Rationale for selection	<i>De facto</i> standard from RSA Security for a request for certification of a public key, a name and an optional set of attributes. Published as an Informational RFC.
Maturity	First published in November 1993. Current version 1.7 was published in 1997. Published as an Informational RFC in November 2000.
Forward outlook	Further development of PKCS standards occurs through mailing list discussions and workshops.

Standard 1 PKCS #10 v1.7 (RFC 2986)	
Version and rationale for version	Version 1.7. Published as an Informational RFC and mature.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
Certificate Request Message Format (CRMF) RFC 2511	<p>CRMF defines a syntax used to convey a request for a certificate to a Certification Authority (CA) (possibly via a Registration Authority (RA)) for the purposes of X.509 certificate production. The request will typically include a public key and associated registration information. CRMF was defined in RFC 2511 in March 1999.</p> <p>CRMF is not widely supported yet. Netscape CMS supports RFC 2511 and Betrusted provides an implementation.</p>

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.10 Certificate profile

Justification for inclusion and usage

Defines the format and semantics of digital certificates to be used within government, to ensure that certificates issued by multiple CAs can be used across government applications.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
RFC 3280 (X.509 v3)	RFC 3280 (X.509 v3)	None

Recommended standards

Standard 1 RFC 3280 (X.509 v3)	
Description	The standard governs the format of X.509 digital certificates.
Rationale for selection	Established IETF Standard for the format of X.509 Version 3 certificate.
Maturity	<p>Originally published as a proposed standard (RFC 2459) in January 1999 and subsequently revised as RFC 3280 in April 2002, it is deemed to be generally stable.</p> <p>RFC 4325 was published in December 2005, which enables the use of the Authority Information Access extension in CRLs, thus enabling a CRL checking application to use the access method (id-ad-caIssuers) to locate certificates that may be useful in the construction of a valid CRL issuer certification path to an appropriate trust anchor.</p>

Standard 1 RFC 3280 (X.509 v3)	
Forward outlook	The IETF Public-Key Infrastructure working group (pkix) will continue to track the evolution of these standards and incorporate changes and additions as appropriate.
Version and rationale for version	RFC 3280 (X.509 v3) is the current standard for certificate profile. RFC 3280 profiles both the X.509 v3 certificate and X.509 v2 CRL for use in the Internet.
Limitations on the use of this standard	It is possible to add proprietary extensions to the X.509 standard format. Such extensions can have a negative impact on interoperability and should be avoided.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.11 Certificate revocation list profile

Justification for inclusion and usage

Defines the format and semantics of certificate revocation lists (CRLs) to enable the status of digital certificates issued by different certification authorities (CAs) to be verified. CRL-based status checking is commonly adopted, although it does not provide the most up-to-date status of a certificate.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
RFC 3280 (X.509 v2)	RFC 3280 (X.509 v2)	None

Recommended standards

Standard 1 RFC 3280 (X.509 v2)	
Description	Use of certificate revocation lists (CRLs) enables organisations to check that a digital certificate has not been cancelled before its natural expiry date. The specification for RFC 3280 develops a profile to facilitate the use of X.509 certificates within Internet applications for those communities wishing to make use of X.509 technology. In order to relieve some of the obstacles to using X.509 certificates, RFC 3280 defines a profile to promote the development of certificate management systems and development of PKI-based application tools.

Standard 1 RFC 3280 (X.509 v2)	
Rationale for selection	RFC 3280 (X.509 v2) is the established, and the only viable Internet standard for profiling X.509 CRLs. RFC 3280 profiles both the X.509 v3 certificate and X.509 v2 CRL for use in the Internet.
Maturity	Originally published as a proposed standard (RFC 2459) in January 1999 and revised as RFC 3280 in April 2002, it is deemed to be generally stable. RFC 4325 was published in December 2005, which enables the use of the Authority Information Access extension in CRLs, thus enabling a CRL checking application to use the access method (id-ad-caIssuers) to locate certificates that may be useful in the construction of a valid CRL issuer certification path to an appropriate trust anchor.
Forward outlook	The IETF Public-Key Infrastructure working group pkix (see http://www.ietf.org/html.charters/pkix-charter.html) will continue to track the evolution of these standards and incorporate changes and additions as appropriate.
Version and rationale for version	RFC 3280 is the current internet standard for profiling X.509 v2 certificate revocation lists.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.12 Certificate import/export interface

Justification for inclusion and usage

Provides a mechanism for storing private keys and certificates and allows for import and export of certificates.

This would allow, for example, users to import certificates provided on diskettes by Certification Authorities or allow certificates to be imported onto tokens or smart cards.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
PKCS #12	PKCS #12 v1.0	None

Recommended standards

Standard 1 PKCS#12 v1.0	
Description	PKCS #12 governs the format used for the export and import of personal identity information.
Rationale for selection	<i>De facto</i> standard from RSA Security for a portable format for storing or transporting a user's private keys, certificates, secrets etc.
Maturity	First published in June 1999.
Forward outlook	Further development of PKCS standards occurs through mailing list discussions and workshops.
Version and rationale for version	Version 1.0. Current version.
Limitations on the use of this standard	None

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.13 Cryptographic token interface

Justification for inclusion and usage

Provides a technology independent programming interface for cryptographic devices such as smart cards and PCMCIA cards used for authentication, authorisation and payment.

Products such as smart card readers, smart cards and cryptographic accelerators should conform to this standard to ensure that it is possible to develop applications which exploit these technologies.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
PKCS #11 Microsoft CryptoAPI	PKCS #11 v2.11 Microsoft CryptoAPI	None
Remarks: Cryptographic tokens not dedicated for a specific purpose should support both interfaces. Applications that use cryptographic tokens may choose to use either of these interfaces.		

Recommended standards

Standard 1 PKCS #11 v2.11	
Description	PKCS #11 defines the interface between applications, such as Web browsers, email clients etc., and devices on which cryptographic operations are performed.
Rationale for selection	<i>De facto</i> standard from RSA Security, PKCS #11 is widely supported by the market leading browsers, software development kits, security tokens and smart card readers.
Maturity	Version 1.0 was published by RSA in April 1995, and v2.11 was published in November 2001. The latest version v2.20 was published on 24 June 2004.
Forward outlook	Further development of PKCS standards occurs through mailing list discussions and workshops. PKCS #11 has undergone a number of iterations since its initial release, indicating that the standard will continue to evolve as requirements dictate.
Version and rationale for version	Version 2.11 is more widely adopted when compared to the more recent version.
Limitations on the use of this standard	None.

Standard 2 Microsoft CryptoAPI	
Description	Microsoft CryptoAPI is a proprietary standard from Microsoft, which is used extensively within Microsoft products to support cryptographic functionality. CryptoAPI provides services that enable application developers to add security based on cryptography to applications. CryptoAPI includes functionality for encoding to and decoding from ASN.1, hashing, encrypting and decrypting data, for authentication using digital certificates, and for managing certificates in certificate stores. Encryption and decryption are provided using both session keys and with public/private key pairs. Import and export of certificates in Internet Explorer, for example, uses CryptoAPI. CryptoAPI is the basis of Microsoft's Internet Security Framework.
Rationale for selection	Mature standard. Required for supporting Microsoft products, such as Internet Explorer - the market leading Internet browser.
Maturity	CryptoAPI was introduced by Microsoft in 1996.
Forward outlook	It is likely that CryptoAPI will remain the dominant standard on Microsoft platforms, as an alternative to PKCS #11.
Version and rationale for version	Not applicable. Microsoft CryptoAPI is provided as part of the core platform SDK and is embedded within appropriate products. CryptoAPI supports Windows 95/98/ME and NT/2000/XP and requires Internet Explorer 3.02 or later.
Limitations on the use of this standard	Specific to Microsoft products.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.14 Cryptographic token information syntax

Justification for inclusion and usage

The use of cryptographic tokens for authentication and authorisation purposes requires a common format for digital credentials and the ability of multiple applications to share such credentials. This will be used by B/Ds to develop authentication and authorisation functionality which is independent of platform or token manufacturer e.g. to allow a user with a token containing a digital certificate to present that certificate to multiple applications for authentication.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
PKCS #15	PKCS #15 v1.1	None

Recommended standards

Standard 1 PKCS #15 v1.1	
Description	PKCS #15 defines the syntax for storing digital credentials (e.g. keys, certificates) on security tokens and how the information can be accessed to enable portability of digital credentials. Complementary to Cryptographic Token Interface standard (PKCS #11).
Rationale for selection	<i>De facto</i> standard from RSA Security, it is the only viable standard.
Maturity	v1.0 published in April 1999. v1.1 published in June 2000.
Forward outlook	Further development of PKCS standards occurs through mailing list discussions and workshops.
Version and rationale for version	v1.1. Current version which is widely adopted by the leading smart card vendors.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.15 Privacy policy

Justification for inclusion and usage

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.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
P3P	P3P v1.0	None

Recommended standards

Standard 1 Platform for Privacy Preferences Project (P3P) v1.0	
Description	P3P enables web sites to express privacy practices in a standardised form that can be automatically retrieved and interpreted by user agents, such as browsers. User agents can compare the privacy practices with the user's preferences and automatically flag differences, allowing the user to respond accordingly.
Rationale for selection	P3P is a W3C recommended standard, and the only viable one available.
Maturity	P3P v1.0 was issued as a W3C recommendation and is thus deemed to be stable and suitable for widespread adoption.
Forward outlook	The P3P Specification Working Group envisions future versions of the specification after 1.0, to incorporate feedback as a result of implementation and deployment and to incorporate a number of components: <ul style="list-style-type: none"> • Allow sites to offer a choice of privacy policies • Allow visitors to explicitly agree, through the user agent, to a policy • A mechanism for non-repudiation of agreements between visitors and sites • A mechanism to transfer user data to services
Version and rationale for version	Version 1.0. W3C Recommendation.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.16 Exchange of authentication and authorisation Information

Justification for inclusion and usage

Required to enable the exchange of authentication and authorisation information across diverse security domains through XML messages.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
SAML	SAML v1.1	WS-Federation
WS-Federation	SAML v2.0	Identity Federation Framework (ID-FF) v1.2
ID-FF		

Recommended standards

Standard 1 Security Assertion Markup Language (SAML)	
Description	Security Assertion Markup Language (SAML) is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.
Rationale for selection	<p>SAML has the following advantages:</p> <p>Platform neutrality. SAML abstracts the security framework away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important tenet of Service-Oriented Architecture.</p> <p>Loose coupling of directories. SAML does not require user information to be maintained and synchronized between directories.</p> <p>Improved online experience for end users. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication. In addition, identity federation (linking of multiple identities) with SAML allows for a better-customized user experience at each service while promoting privacy.</p> <p>Reduced administrative costs for service providers. Using SAML to 'reuse' a single act of authentication (such as logging in with a username and password) multiple times across multiple services can reduce the cost of maintaining account information. This burden is transferred to the identity provider.</p> <p>Risk transference. SAML can act to push responsibility for proper management of identities to the identity provider, which is more often compatible with its business model than that of a service provider.</p>

Standard 1 Security Assertion Markup Language (SAML)	
Maturity	SAML had been formulated as open standard by vendors to address cross-enterprise Web Single Sign-On, and the exchange of security information between security domains. The major version is v1.0 approved as OASIS standard in November 2002. Approval of SAML v1.1 followed in September 2003, when XML Signature was introduced to SAML specifications. The latest version, SAML v2.0, was officially approved as an OASIS standard in March 2005.
Forward outlook	Various efforts to build profiles and related specifications on top of SAML v2.0 are proceeding. There are other related standards such as Liberty Alliance ID-FF and ID-WSF that will extend some of the functions of SAML.
Version and rationale for version	<p>SAML v1.1 is a mature standard and has already gained wide industry support. The latest version, SAML v2.0, was officially approved as an OASIS standard in March 2005. It introduces a number of new features, including:</p> <ul style="list-style-type: none"> ● Pseudonyms (a key privacy-enabling technology) ● Identifier management (for managing pseudonyms) ● Metadata (for expressing configuration and trust-related data to make deployment of SAML systems easier) ● Encryption (so that attribute statements, name identifiers, or entire assertions can be encrypted in place) ● Attribute profiles ● Session management (for single logout) ● Mobile device support (to better address their challenges and opportunities) ● Identity provider discovery (for deployments having more than one identity provider) <p>A number of organizations (including Oracle, Novell, Trustgenix [acquired by HP], Symlabs and Sun Microsystems) have demonstrated interoperability of products and solutions that incorporate the SAML v2.0 standard specifications.</p>
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
WS-Federation	<p>WS-Federation 1.0 specification dated July 2003 is an initial public draft released for review and evaluation only. It is backed by some major IT players such as IBM, Microsoft, BEA, Verisign and RSA Security. It is part of an overall effort from IBM and Microsoft to build a Web Services security framework, or WS-Security.</p> <p>According to the specification, the specific goals of WS-Federation are: "Enable appropriate sharing of identity, authentication, and authorization data using different or like mechanisms; brokering of trust and security token exchange; local identities are not required at target services; optional hiding of identity information and other attributes."</p> <p>WS-Federation has three functional parts, including the Web Services Federation Language, which defines how different security realms broker identities, user attributes and authentication between Web Services. The specification also includes Passive Requestor Profile, which describes how federation helps provide identity services to HTTP 1.1-based Web browsers, Web-enabled cell phones and devices; and Active Requestor Profile, which does the same for applications based</p>

	<p>on Simple Object Access Protocol and other smart clients.</p> <p>WS-Federation is a building block that is used in conjunction with other Web Services and application-specific protocols to accommodate a wide variety of security models. The specification describes a model for authentication which builds on the foundations specified in WS-Security, WS-Policy, and WS-Trust.</p> <p>It is observed that some products have been deploying the technology (WS-Federation as an underneath standard) that enables users and applications to interact with InfoCard-compatible Web sites and services. Such products include the 'DigitalMe' of Novell, 'Tivoli Federated Identity Manager' of IBM and Microsoft CardSpace. However, extensive adoption in the market, major project implementations and interoperability amongst different products remain to be seen.</p>
Identity Federation Framework (ID-FF) v1.2	<p>ID-FF is a set of specifications developed by the Liberty Alliance Project that was formed to establish an open standard for federated network identity. The specification aims to enable:</p> <ul style="list-style-type: none"> ● Businesses to create new relationships with each other and to realize business objectives quicker, more securely and at a lower cost. ● Businesses to more easily and securely provision accounts and provide access to the right resources. ● Consumers and employees to have a far more satisfactory on-line experience as well as new levels of personalization, security and control over identity information. <p>Product support on ID-FF v1.2 are emerging. Liberty Alliance's membership involves multiple industry sectors other than IT. This composition gives it a distinct advantage of broad adoption across multiple industry sectors. Its acceptance and adoption in the market should be further observed.</p>

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.1.17 Time stamping protocol

Justification for inclusion and usage

Required to utilise a trusted third party time stamping authority (TSA) to establish evidence that data existed at a particular point in time and could be used by an application for non-repudiation purposes or to prove that data was signed before a certificate was revoked.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
RFC 3161 (X.509 PKI TSP)	RFC 3161 (X.509 PKI TSP)	None

Recommended standards

Standard 1 RFC 3161 (X.509 PKI TSP)	
Description	RFC 3161 defines the format of a request sent to a Time Stamping Authority (TSA) and that of the response that is returned. It also defines security-related requirements for TSA operation with regard to processing requests and generating responses.
Rationale for selection	RFC 3161 is the only viable standard.
Maturity	It is an established IETF Standard published in August 2001 and is generally stable.
Forward outlook	The IETF Public-Key Infrastructure working group (pkix) will continue to track the evolution of the standard and incorporate changes and additions as appropriate.
Version and rationale for version	RFC 3161 is the current internet standard for time stamping protocol.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.3.2 Interoperability areas for future consideration – standards not matured yet

3.3.2.1 XML-based authorisation and entitlement

Justification for inclusion and usage

Required to enable the XML representation of authorisation and entitlement policies.

Standards for future consideration

Standard(s)	Description
XACML	eXtensible Access Control Markup Language (XACML) is an XML-based language for access control that is standardized in OASIS. XACML describes both an access control policy language and a request/response language. The policy language is used to express access control policies (who can do what and when). The request/response language expresses queries about whether a particular access should be allowed (requests) and describes answers to those queries (responses). XACML Version 2.0 has been ratified as an OASIS standard in February 2005. Standards in this area are not widely adopted yet so this area has been classified for future consideration.

3.3.2.2 XML key management

Justification for inclusion and usage

Required to enable XML-based clients to obtain cryptographic keys necessary for XML signing and encryption, including those from existing PKI infrastructures, through support for key registration, location and validation.

Standards for future consideration

Standard(s)	Description
XKMS	XML Key Management Specification (XKMS) is developed under the XKMS Activity of W3C, which started in December 2001. The standard is required to enable XML-based clients to obtain cryptographic keys necessary for XML Signature and XML Encryption, including those from existing PKI infrastructures. XKMS supports registration, location and validation of keys through two standards: XML Key Registration Service Specification (X-KRSS) for registration and XML Key Information Service Specification (X-KISS) for location and validation. XKMS Version 2.0 has been published as a W3C Recommendation on 28 June 2005. Standards in this area are not widely adopted yet so this area has been classified as for future consideration.

3.4 INTERCONNECTION DOMAIN

3.4.1 Interoperability areas for immediate consideration

3.4.1.1 E-mail transport

Justification for inclusion and usage

Required to enable the sending of e-mail messages between mail servers and from e-mail clients to mail servers. E-mail products must support interfaces that conform to the e-mail transport standards.

Relevant to submissions under ETO : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
SMTP	SMTP (RFCs 2821, 2822)	None

Recommended standards

Standard 1 Simple Mail Transport Protocol (SMTP) (RFCs 2821 and 2822)	
Description	The objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently. SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel. RFC 2822 (April 2001) is complementary to RFC 2821, defining the protocol for standard text messages that are sent via SMTP.
Rationale for selection	Globally recognised, mature IETF standard. Complementary to MIME, and widely adopted.
Maturity	Created in 1982 (as Standard RFC 821), SMTP was widely adopted by 1996.
Forward outlook	Although SMTP is a robust standard, the need for a number of protocol extensions is evident. Several extensions were suggested in 1995, though these have not yet been widely adopted as the original simplicity of SMTP has been its success.
Version and rationale for version	Currently only one version of SMTP exists, as defined by RFCs 2821 and 2822.
Limitations on the use of this standard	RFC 2821/2822 mail systems do very well for text messages sent in US-ASCII, and fall within the limitation of 1000 characters or less per line. However, for international character sets, or image files, this system does not work. Another limitation is the possible loss of information when a message is transferred between X.400 and RFC 2822 hosts. When an X.400 message is mapped to a RFC 2822 host, any non textual information must be converted to IA5 text, or be discarded. These limitations are addressed by multipurpose internet mail extensions (MIME) which enables the exchange of different types of data files.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.4.1.2 Mail box access

Justification for inclusion and usage

Required to enable remote access to e-mail boxes. E-mail products must provide remote mailbox access that conforms to the mail box access standards.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
POP3 IMAP4	POP3 - for basic mail box access IMAP4 rev1 - for more advanced functionality allowing clients to manipulate messages on the server	None

Recommended standards

Standard 1 Post Office Protocol v3 (POP3)	
Description	POP3 is a client/server protocol in which e-mail is received and held on a mail server. Periodically, the mail-box on the server is checked and any mail downloaded.
Rationale for selection	Mature, IETF standard. The Post Office Protocol version 3 [POP3] is very widely used.
Maturity	Version 3 – (RFC 1939). Mature standard introduced in 1996. RFC 1939 was updated by RFC 2449 in November 1998.
Forward outlook	POP3 will remain a dominant standard for remote mailbox access.
Version and rationale for version	Version 3 as defined in RFCs 1939 and 2449. Mature standard introduced in 1996 and updated in November 1998.
Limitations on the use of this standard	None.

Standard 2 Internet Message Access Protocol Version 4 (IMAP4) rev1	
Description	IMAP4 is a proposed IETF standard defined in RFC 3501. IMAP4 allows a client to access and manipulate electronic mail messages on a server. IMAP4 permits manipulation of remote message folders, called “mailboxes”, in a way that is functionally equivalent to local mailboxes. IMAP4 also provides the capability for an offline client to resynchronise with the server. 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.
Rationale for selection	IMAP4 is a mature IETF standard which is well supported by the major mail clients and servers. Required to support more advanced mail client functionality, such as synchronisation between client and server, fetching of mail headers with optional downloading of mail headers and sophisticated message searching.
Maturity	The original IMAP specification (RFC 1730) was published in 1994 and was obsoleted by RFC 2060 in 1996, which was then obsoleted by the current specification (RFC 3501) in 2003.
Forward outlook	IMAP4 will remain a dominant standard for remote mailbox access.
Version and rationale for version	Version 4 rev1 as defined by RFC 3501.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.4.1.3 Hypertext transfer protocol

Justification for inclusion and usage

Hypertext transfer protocol defines how messages are formatted and transmitted and the commands used by servers and clients, for example, to enable browser-based access to hypertext content and transfer of SOAP message over HTTP.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
HTTP	HTTP/1.1	None

Recommended standards

Standard 1 HyperText Transfer Protocol HTTP/1.1	
Description	HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. In relation to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.
Rationale for selection	HTTP has been in use by the World Wide Web global information initiative since 1990. It is a global, mature and widely adopted standard.
Maturity	HTTP has been in use by the World Wide Web global information initiative since 1990.
Forward outlook	Both HTTP extensions and HTTP/1.1 are stable specifications, W3C has closed the HTTP Activity. The Activity has achieved its goals of creating a successful standard that addresses the weaknesses of earlier HTTP versions. HTTP/1.1 is likely to have general use along with web applications.
Version and rationale for version	HTTP/1.1 is currently the most widely used and latest version of this standard. (RFC 2616).
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.4.1.4 Directory access

Justification for inclusion and usage

Required to access information stored in a standard directory. Standard directories provide a centralised or distributed repository of organisation, organisational units (divisions, departments etc), people, IT resources e.g. printers, together with associated attributes e.g. user name, printer name, e-mail address etc. The directory access protocol defines how to locate information in such directories.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
LDAP DAP	LDAP v3	None

Recommended standards

Standard 1 Lightweight Directory Access Protocol (LDAP) v3	
Description	The protocol is designed to provide access to X.500 or other directories with less resource usage than Directory Access Protocol (DAP). This protocol is specifically targeted at simple management applications and browser applications that provide simple read/write interactive access to a directory.
Rationale for selection	IETF standard introduced in 1997. Dominant directory access protocol supported by all the major directory software providers.
Maturity	Introduced in 1993 (RFC 1487) and then updated/obsoleted by RFC 1777 in March 1995. Version 3 (RFC 2251) was introduced in 1997.
Forward outlook	Several updates have already been implemented on top of the original scope and it is likely that more updates/new versions will be introduced in future.
Version and rationale for version	Version 3 is the latest version and has been widely adopted.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
DAP	<p>Directory Access Protocol (DAP) is a well-established standard introduced in 1991. The X.500 protocol (which covers DAP) is covered by a series of RFCs covering the schema, implementation, technical overview and advanced usages of the standard. (See RFC numbers 1274, 1276, 1308, 1309, 1491 and 2116).</p> <p>DAP may not be applicable to non X.500 compliant directories. Since LDAP is functionally sufficient for accessing directories, is commonly supported by all directory servers and is not as resource intensive, it is recommended in preference to DAP.</p> <p>There is limited activity in progressing the DAP specifications.</p>

3.4.1.5 Domain name service

Justification for inclusion and usage

Required for locating 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 which maps those names to Internet addresses. For example, www.gov.hk is the domain name of a server which handles World Wide Web requests (indicated by the www), for a government organisation (indicated by the gov) in Hong Kong (indicated by the hk) and maps to the Internet address 202.128.227.75. When a user enters a URL which begins with www.gov.hk, a domain name server uses the domain name service to determine the Internet address to send the request to.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
DNS	DNS	None
IDN	IDN	

Recommended standards

Standard 1 Domain Name System (DNS)	
Description	<p>The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.</p> <p>Maintaining a central list of domain name or IP address mappings would be impractical, and so they are distributed throughout the Internet based on a hierarchical model.</p>
Rationale for selection	Extremely mature, globally adopted standard.
Maturity	Introduced in 1987 (RFC 1034 and RFC 1035), therefore a very mature standard.
Forward outlook	Historically, DNS has been extended to enhance interoperability. It is likely that similar extensions will be added in the future.

Standard 1 Domain Name System (DNS)	
Version and rationale for version	As defined in: RFC 1034 and updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC2065, RFC2181, RFC2308, RFC2535. RFC 1035 and updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC1995, RFC1996, RFC2065, RFC2136, RFC2181, RFC2137, RFC2308, RFC2535, RFC2845.
Limitations on the use of this standard	None.

Standard 2 Internationalized Domain Name (IDN)	
Description	An IETF standard for multilingual domain names. In simple words, IDN is a domain name presented in native languages. It contains non-ASCII character string, and involves the domain name conversion method between ASCII and non-ASCII characters, a fundamental requirement of not disrupting the operation of DNS.
Rationale for selection	HKDNR has already approved the registration of 2600+ Chinese domain names (CDN), among which there are more than 100 government domain names.
Maturity	Standardized in 2003 (RFC3490, RFC3491 and RFC3492) and latest version of Internet browser software generally support CDN.
Forward outlook	ICANN has a roadmap for the introduction of IDN based on current and future work.
Version and rationale for version	As defined in RFC 3454, RFC3490, RFC3491, RFC3492 and RFC3743, "Guidelines for the Implementation of Internationalized Domain Names" issued by ICANN.
Limitations on the use of this standard	Latest version of Internet browser software generally supports CDN. There is also some free plug-in software for the prior version of respective Internet browser supporting the use of CDN.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.4.1.6 File transfer

Justification for inclusion and usage

Required to enable transfer of files over TCP/IP e.g. to enable a user to download content from a central server, or to transfer files between two servers.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
FTP	FTP	None
HTTP	HTTP/1.1	
SFTP	SFTP	
<p>Remarks:</p> <p>The FTP and HTTP protocol on their own have no provision for data encryption. Project teams demanding data encryption may use SFTP or use FTP/HTTP over a secure channel to enable secure file transfer.</p> <p>For server-to-client secure file transfer in a Web-based environment, the simplest way is to use HTTP over SSL/TLS to avoid having to install client-side software.</p>		

Recommended standards

Standard 1 File Transfer Protocol (FTP)	
Description	File Transfer Protocol (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols.
Rationale for selection	Extremely mature, globally adopted standard.
Maturity	First introduced in 1971(RFC114) and formalised as a standard in 1985 (STD0009).
Forward outlook	FTP over SSL/TLS (ftps) can be used for secure file transfer between computers. It is an extension to FTP that adds security and authentication using SSL/TLS protocol, and it conforms to RFC2228. Products that support FTP over SSL/TLS are already available.
Version and rationale for version	Currently only one version exists.
Limitations on the use of this standard	None.

Standard 2 HyperText Transfer Protocol HTTP/1.1
Please refer to the area "Hypertext transfer protocol" for details on HTTP/1.1

Standard 3 SSH File Transfer Protocol (SFTP)	
Description	SSH File Transfer Protocol (SFTP) is a file transfer protocol that allows the secure transfer of files between two computers. SFTP relies on Secure Shell (SSH) for authenticating users in a secure manner. sftp and scp, similar to ftp and rcp respectively, are commonly found client programs that implements SFTP. Most SSH version 2 (SSH2) products provides both sftp and scp.
Rationale for selection	sftp and scp are widely adopted for transferring files securely in UNIX and Linux environments. Open source implementation is available.

Standard 3 SSH File Transfer Protocol (SFTP)	
Maturity	SFTP was first introduced in Secure Shell version 2 (SSH2) which was released in 1997 by SSH Communications Security. SFTP has become a de-facto industry standard used by all major UNIX and Linux OS vendors, and independent distributions are also available for Windows.
Forward outlook	SFTP is likely to remain as a popular secure file transfer protocol in the market. As for SSH2, it was submitted as an Internet Engineering Task Force (IETF) draft in 1997 and is still being standardized by the IETF Secure Shell Working Group.
Version and rationale for version	As defined in the latest IETF specifications. Current specification can be found in http://www.ietf.org/proceedings/04aug/I-D/draft-ietf-secsh-filexfer-05.txt .
Limitations on the use of this standard	SFTP is not yet supported by Microsoft Windows and additional software is required to provide sftp/scp features for Windows.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.4.1.7 LAN/WAN interworking

Justification for inclusion and usage

Required to allow data to be sent from one computer to another on a local area network (LAN) or wide area network (WAN), based on the computer's unique address on the network.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
IPv4	IPv4	None
IPv6	IPv6	

<p>Remarks:</p> <p>IPv4 hosts are unable to communicate directly with IPv6 hosts, and vice versa. Solutions based on upper layers of network protocols are required for interoperability between IPv4 and IPv6 hosts.</p> <p>IPv4 and IPv6 are expected to co-exist for a long period of time due to the prominent role IPv4 is currently playing. Project teams are highly advised to select products that support or with roadmap to support IPv6 in addition to IPv4.</p>

Recommended standards

Standard 1 Internet Protocol (IP) v4	
Description	The Internet Protocol (IP) is the protocol by which data is sent between interconnected systems of packet-switched computer communication networks, including LANs, WANs and the Internet. Each computer (known as a host) has at least one IP address that uniquely identifies it from all other computers. When data is sent or received (for example, an e-mail note or a Web page), the message is divided into packets. Each of these packets contains both the sender's IP address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the network. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the network until one gateway recognises the packet as belonging to a computer within its immediate neighbourhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.
Rationale for selection	Mature, globally adopted standard, which is supported extensively.
Maturity	The transition to IPv4 took place in 1983, so a mature standard that has been in place globally for over 20 years.
Forward outlook	IPv4 will coexist with IPv6 for a period of time.
Version and rationale for version	Version 4 is the current and most widely used version of IP. This version has been in place for over 20 years and is therefore a very mature standard.
Limitations on the use of this standard	The most significant limitation of IPv4 is the number of addresses which can be supported.

Standard 2 Internet Protocol v6	
Description	IPv6 was formalized in 1998. It provides for much longer addresses and therefore enable the possibility of many more Internet addresses to support more users, servers etc. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.
Rationale for selection	The Internet backbone of the local universities has already been upgraded to a high-speed network of 10 giga-bit-per-second in support of IPv6. The Government will also take the lead to adopt the new protocol in the Government's internal network by 2008.
Maturity	Introduced in 90's (RFC 1752 and RFC 2462), most of the operating systems, networking and application products support IPv6 to a certain extent.
Forward outlook	IPv4 and IPv6 will coexist for a period of time.
Version and rationale for version	Comparing with the IPv4 specification, IPv6 makes improvements such as vast address space, embedded security, simpler mobility and auto-configuration.

Limitations on the use of this standard	Users shall evaluate the security products, which are still not so common in the market.
--	--

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.4.1.8 LAN / WAN transport protocol

Justification for inclusion and usage

Works in conjunction with LAN/WAN interworking protocols to allow data to be sent from one computer to another on a LAN or WAN.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
TCP	TCP – preferred transport protocol over UDP	None
UDP	UDP – where required e.g. to support particular protocols	

Recommended standards

Standard 1 Transmission Control Protocol (TCP)	
Description	<p>Transmission Control Protocol (TCP) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. 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 Internet.</p> <p>TCP, in contrast to UDP, is a connection-oriented protocol meaning that a virtual circuit is established between the two computers and ensures that packets are received in the same order in which they are transmitted. TCP also notifies the application if the connection between the two computers fails.</p>
Rationale for selection	Mature, global, and widely adopted standard.
Maturity	Introduced in 1991.
Forward outlook	Not likely to change as TCP is in the Transport layer providing a way of assembling packets of data at their destination and as long as IP is in use this will be the case.

Standard 1 Transmission Control Protocol (TCP)	
Version and rationale for version	Currently only one version exists.
Limitations on the use of this standard	None.

Standard 2 User Datagram Protocol (UDP)	
Description	UDP is an alternative to TCP. UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP is a connectionless protocol and so does not divide a message into packets (datagrams) and reassemble it at the other end or guarantee that messages will arrive at the destination in the correct sequence. This means that an application program which uses UDP must be able to make sure that the entire message has arrived and is in the right order. These characteristics of UDP mean that it cannot be relied on for data delivery. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP.
Rationale for selection	Mature IETF standard.
Maturity	The UDP specification is detailed in RFC 768, filed in 1980.
Forward outlook	TCP is likely to be adopted in preference to UDP as it is more efficient at processing large volumes of data.
Version and rationale for version	As defined by RFC 768.
Limitations on the use of this standard restrictions)	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	

3.4.1.9 Wireless LAN

Justification for inclusion and usage

Required to support mobile access to LANs. The users of wireless LANs (WLANs) may, subject to whether there is security concern over the information being transmitted over the WLAN, apply some security solutions to better assure the integrity and confidentiality of the information transmitted over the WLAN.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
IEEE 802.11b IEEE 802.11g IEEE 802.11a IEEE 802.11n	IEEE 802.11b IEEE 802.11g	IEEE 802.11n
<p>Remarks:</p> <p>Products of Wireless LAN with Wi-Fi Certification are recommended in order to ensure the interoperability between different manufacturers.</p> <p>All new access points are highly recommended to support IEEE 802.11g. New client devices are also recommended to support IEEE 802.11g where possible.</p>		

Recommended standards

Standard 1 Institute of Electrical and Electronics Engineers (IEEE) 802.11 b/g	
Description	<p>IEEE 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). There are currently 13 specifications in the family: from IEEE 802.11a to IEEE 802.11ma.</p> <p>IEEE 802.11b, and IEEE 802.11g are two specifications that define complete wireless LAN systems in 2.4GHz frequency band.</p>
Rationale for selection	Both IEEE 802.11b and IEEE 802.11g are mature and widely adopted standards.
Maturity	<p>IEEE 802.11 accepted by the IEEE in 1997.</p> <p>IEEE 802.11b was ratified in 1999 and IEEE 802.11g was ratified in 2003.</p>
Forward outlook	New amendments will be added to the IEEE 802.11 family to increase the throughput by technology breakthrough.
Version and rationale for version	<p>IEEE 802.11b is widely adopted in market in all formats.</p> <p>IEEE 802.11g is backward compatible with IEEE 802.11b with higher throughput and will finally replace IEEE 802.11b and be prevalent in the 2.4GHz frequency band market.</p>
Limitations on the use of this standard	<p>There are known security problems with all of the IEEE 802.11 standards.</p> <p>Congestion in the 2.4GHz band (2.4GHz frequency band is also used by Bluetooth, RFID, wireless keyboard/mouse, microwave oven, etc.) is a potential drawback to the IEEE 802.11b and IEEE 802.11g standards.</p>

Emerging standards for future consideration

Emerging Standard(s)	Description
IEEE 802.11n	<p>IEEE 802.11n is a proposed amendment to the IEEE 802.11 to significantly improve network throughput over 802.11b and 802.11g, with a significant increase in the maximum raw (PHY) data rate from 54 Mbit/s to a maximum of 600 Mbit/s. Products of IEEE 802.11n draft 2.0 are widely available in Hong Kong market to fulfill consumer requirement for wireless networking with higher throughput before IEEE 802.11n finalized (802.11n is expected to be finalized in November 2009). Products supporting IEEE 802.11n draft 2.0 are relatively more expensive than IEEE 802.11 b/g and consume more power, limiting its usability in the mobile market.</p>

Other Candidate Standards

Other Standard(s)	Description
IEEE 802.11a	<p>IEEE 802.11a is a specification that defines complete wireless LAN systems that operate in 5GHz frequency band and was ratified by IEEE in 1999.</p> <p>It provides high speed wireless access with up to 24 non-overlapping channels in the 5GHz frequency band. Unlike IEEE 802.11b/g, this 5GHz band is less susceptible to interference, and IEEE 802.11a in general provides higher throughput than IEEE 802.11g.</p> <p>Products of IEEE 802.11a are available in Hong Kong market since the official regulation of 5GHz frequency band by OFTA in Feb 2003. (See http://www.ofta.gov.hk/legislation/class-licence/wlan_lic.pdf).</p> <p>Most of the latest high-end WLAN products support multiple standards (IEEE 802.11a, plus IEEE 802.11b and/or IEEE 802.11g) in order to provide users more flexibility for wireless connection in both 2.4 GHz and 5 GHz frequency bands.</p> <p>Major implementations of IEEE 802.11a are currently in the enterprise market. Products supporting IEEE 802.11a are relatively more expensive than IEEE 802.11b/g and not widely adopted in low-end market.</p>

3.4.1.10 Wireless LAN security

Justification for inclusion and usage

User should adopt this interoperable standard for secure wireless local area network (WLAN) access should RF level security be required.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
WPA WEP WPA2	WPA WPA2	None
<p>Remarks:</p> <p>In addition to WPA, WPA2 provides a stronger encryption mechanism through AES, which is a requirement for some corporate and government users.</p>		

Recommended standards

Standard 1 Wi-Fi Protected Access (WPA)	
Description	<p>WPA is a standard-based, interoperable security technology for Wi-Fi networks. It provides data protection by using encryption as well as access control and user authentication.</p> <p>WPA includes 802.1X and TKIP technology. Cryptographers working with the Wi-Fi Alliance have reviewed WPA and endorsed the fact that it solves all known vulnerabilities of Wireless Equivalent Privacy (WEP).</p>

Standard 1 Wi-Fi Protected Access (WPA)	
Rationale for selection	WPA is one of the wireless security standards, which is commonly available in the WLAN products. WPA was independently verified to address all of WEP's known weaknesses while the release of WPA2 is not used to address any flaws in WPA.
Maturity	WPA was announced in October 2002. Wi-Fi certified products are common in the market. Nowadays, most of the WLAN products including clients and access points support WPA because WPA has been the mandatory requirement for Wi-Fi certification since August 2003.
Forward outlook	Wi-Fi certification for WPA2 was launched in September 2004. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is backward compatible with WPA.
Version and rationale for version	N/A
Limitations on the use of this standard	None.

Standard 2 Wi-Fi Protected Access (WPA2)	
Description	WPA2 is a standard-based, interoperable security technology for Wi-Fi networks. It provides data protection by using encryption as well as access control and user authentication. WPA2 is the approved Wi-Fi Alliance interoperable implementation of 802.11i. WPA2 utilize 802.1X and Extensible Authentication Protocol (EAP) for authentication. WPA has Personal and Enterprise modes of operation to address the needs of the consumer and enterprise market segments. Cryptographers working with the Wi-Fi Alliance have reviewed WPA2 and endorsed the fact that it provide security that can meet the FIPS 140-2 requirement.
Rationale for selection	In addition to WPA, WPA2 provides a stronger encryption mechanism through AES, which is a requirement for some corporate and government users.
Maturity	The first set of products that have been Wi-Fi Certified for WPA2 was announced in September 2004. Wi-Fi certified products with both WPA and WPA2 are common in the market. Nowadays, most of the WLAN products including clients, access points, wireless switches support WPA and WPA2. WPA2 is backward compatible with WPA.
Forward outlook	
Version and rationale for version	N/A
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
WEP	<p>WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.</p> <p>WEP has not been selected because serious security flaws were found in the protocol. For details, refer to http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.</p>

3.4.1.11 Mobile device Internet access

Justification for inclusion and usage

Required to support Internet-based access from mobile devices, such as mobile phones and PDAs, enabling users to obtain access to Internet-based content provided by Government.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
WAP	WAP v2.0 – for use with WAP devices	None
HTTP	HTTP v1.1 – for use with mini-browser	

Recommended standards

Standard 1 Wireless Application Protocol (WAP) v2.0	
Description	<p>The WAP specification initiative began in June 1997 and the WAP Forum, a cross-industry group, was founded in December 1997 to define the WAP specification to enable manufacturers, network operators, content providers and application developers to offer compatible products and secure services on all devices and networks.</p> <p>WAP (Wireless Application Protocol) is a specification for a set of communication protocols to standardise the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC).</p> <p>WAP 2.0 provides managed backward compatibility to existing WAP content, applications and services that comply with previous WAP versions. Besides, WAP 2.0 adds new and enhanced services such as WAP Push, User Agent Profile, Wireless Telephony Application, Data Synchronization, MMS and WAP 2.0 stack (support end-to-end security). (Note that from 12 June 2002, a new group, the Open Mobile Alliance, now controls WAP standards http://www.openmobilealliance.org/pr2002-06-12.html).</p>
Rationale for selection	<p>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.</p>
Maturity	<p>WAP version 1.0 specification was approved in 1998. WAP version 1.2 was approved by the WAP Forum in November 1999. WAP 1.2.1 was approved in June 2000. WAP 2.0 was officially released in January 2002.</p>

Standard 1 Wireless Application Protocol (WAP) v2.0	
Forward outlook	WAP standards will continue to be developed by the Open Mobile Alliance.
Version and rationale for version	<p>v2.0 is a mature version which is supported by mobile devices, microbrowsers and WAP servers from the leading vendors. WAP 2.0 provides managed backward compatibility to existing WAP content, applications and services that comply with previous WAP versions.</p> <p>WAP 2.0 provides support for both WAP 1.x stack and WAP 2.x stack, and both stacks would operate independently. That is, there would not be mixing and matching of protocols in accomplishing an end-to-end transaction.</p> <p>Backward compatibility is not mandatory in WAP 2.0. Based on business requirements and depending on the target users, project teams may choose WAP proxies and devices that support both stacks in order to provide connectivity model on a broader range of networks, content and wireless bearers.</p>
Limitations on the use of this standard	None.

Standard 2 HTTP v1.1
Please refer to the area “Hypertext Transfer Protocol” for details on HTTP v1.1

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other Candidate Standards

Other Standard(s)	Description
None	