Digital Policy Office

Analysis Underpinning the Recommendations on Interoperability Framework for e-Government

Version: 23.0

December 2024

The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

COPYRIGHT NOTICE

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

Prepared By: Interoperability Framework Coordination Group

Document Effective Date: 1 March 2025

Amendment History				
Change Number	Revision Description	Sections Affected	Revision Number	Date
	Major updates to version 22.1 issued in July 2024 are as follows:		23.0	December 2024
1.	Add OpenAPI v.3.1 as Recommended Standard under the interoperability area of "Simple functional integration in an open environment" in the Application Integration Domain.	3.1.2.1		
2.	Replace PKCS #12 v1.0 with PKCS #12 v1.1 in Recommended Standard under the interoperability area of "Certificate import/export interface" in the Security Domain.	3.3.1.17		
3.	Upgrade Domain Name System Security Extensions (DNSSEC) from Standard for future consideration to Recommended Standard under the interoperability area of "Domain name system (DNS) security" in the Security Domain.	3.3.1.24 3.3.2.4 (deleted)		

TABLE OF CONTENTS

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 Interoperability Framework for e-Government[1] 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 welcome, and comments should be sent to the Interoperability Framework Co-ordination Group (IFCG) (ifcg@digitalpolicy.gov.hk).

The abbreviation HKSAR will be used to stand for the Hong Kong Special Administrative Region of the People's Republic of China throughout this document.

[1] Internet:
https://www.digitalpolicy.gov.hk/en/our_work/infrastructure/e_government/if/interoperability_framework.htm

Intranet: https://itginfo.ccgo.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 Innovation, Technology and Industry 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 realise 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.

There are several commonly adopted streams of application integration standards, namely:

- ebXML;
- Web Services based around a core set of standards: SOAP, WSDL and UDDI;
- Open Virtualization Format (OVF);
- Content Management Interoperability Services (CMIS); and
- Asynchronous message exchange protocol standards: AMQP and MQTT.

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 customisation) may be necessary if a project needs to mix the use of standards from these 2 suites.

The Open Virtualization Format (OVF) specification describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines. It is submitted by leading virtualisation companies to the Distributed Management Task Force (DMTF) 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. Version 1.1.0 released in January 2010 was the mature version supported by vendors. This OVF standard was approved and published as ISO/IEC 17203:2011 in December 2011, its second edition was published as ISO/IEC 17203:2017 in September 2017. The latest version is OVF 2.1.1 which was released in August 2015.

Content Management Interoperability Services (CMIS) is an open standard for improving interoperability between content management systems and repositories. CMIS defines an abstraction layer for controlling diverse content management systems and repositories using Web protocols. A domain model and three protocol bindings including Restful AtomPub binding (RFC 5023), Web Services binding (WSDL) and browser binding (Java Script Object Notation, JSON, RFC 4627) are defined for applications to communicate with content management systems and repositories in a vendor-neutral format. CMIS v1.0 was approved as an OASIS standard on 1 May 2010. The latest version 1.1 was approved as an OASIS standard on 23 May 2013.

Asynchronous message exchange between application systems defines specifications for applications to exchange messages asynchronously to facilitate the development and integration of applications handling large number of devices. Currently, there are two commonly adopted protocols, Advanced Message Queuing Protocol (AMQP) and Message Queue Telemetry Transport (MQTT).

AMQP is an open standard for passing business messages between applications or organisations. It connects systems, feeds business processes with the information they need and reliably transmits onward the instructions that achieve their goals. AMQP version 1.0 specification was approved by the Organization for the Advancement of Structured Information Standards (OASIS) in October 2012. AMQP version 1.0 was approved for release by ISO/IEC in April 2014 and given the designation ‘ISO/IEC 19464’.

MQTT is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. MQTT version 3.1.1 specification was approved by the OASIS in 2014. MQTT version 3.1.1 was approved for release by ISO/IEC in June 2016 and given the designation ‘ISO/IEC 20922’. On 7 March 2019, the OASIS published the official MQTT version 5.0 with significant updates (which supersedes the existing version 3.1.1). However, the maturity and adoption by the industry has yet to be confirmed.

In recent years, Web applications adopting the REpresentational State Transfer (REST) style of software architecture for integration among distributed applications and clients are becoming more popular. The REST architectural style describes six constraints applied to the architecture, while leaving the implementation of the individual components free to design. Conforming to the REST constraints is generally referred to as being "RESTful". Being an architecture style for designing networked applications rather than a protocol such as SOAP, REST itself is not a candidate for inclusion under the IF. However, specifications adopting the REST architectural style can be included as IF specifications wherever appropriate.

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 OpenAPI CORBA DCOM RMI WSIL	The suite of core Web Services standards: - SOAP v1.1 or SOAP v1.2 for remote service invocation - WSDL v1.1 or WSDL v2.0 for remote service description - (where necessary) UDDI v2 or UDDI v3.0.2 for the publication and discovery of remote service descriptions OpenAPI v3.0 or v3.1	None
Remarks: When project teams select products to implement Web Services, they are recommended to take into consideration the products' conformance to the Web Services Basic Reliable and Secure Profiles's (WS-BRSP) Basic Profile v1.1, Basic Profile v1.2 or Basic Profile v2.0. In addition, project teams should implement their Web Services requests and responses in accordance with the version of WS-BRSP Basic Profile they choose. W3C has not yet announced further development for WSDL v2.0.		

Recommended standards

Standard 1a Simple Object Access Protocol (SOAP) v1.1 or SOAP v1.2	
Description	Simple Object Access Protocol (SOAP) v1.1 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

Standard 1a Simple Object Access Protocol (SOAP) v1.1 or SOAP v1.2	
	messages to provide more sophisticated interactions, including remote procedure calls (RPCs) and conversational document exchange. SOAP messages can be exchanged using a variety of protocols, including application layer protocols, such as HTTP and SMTP. SOAP does not define data semantics, message routing, reliable data transfer etc. In summary, SOAP provides an extensible framework for application-to-application integration, capable of supporting a variety of integration scenarios incorporating new and existing applications. SOAP v1.2 has better support for Web standards. It also takes into account internationalisation issues that are inherent to the World Wide Web. SOAP v1.2 uses existing, established Web technologies for improved performance and is truly protocol independent, which means that SOAP v1.2 messages could be carried by HTTP, SMTP, or any other protocol for which a binding conforms to the HTTP binding framework.
Rationale for selection	SOAP v1.1 is one of the core technologies which underpins Web Services and has significant industry support from a broad range of infrastructure and application providers. SOAP v1.2 provides a more specific definition of the SOAP processing model that removes many of the ambiguities that might lead to interoperability errors in the absence of the WS-BRSP profiles. The goal is to significantly reduce the chances of interoperability issues between different vendors that use SOAP 1.2 implementations. Both SOAP v1.1 and SOAP v1.2 are included in the WS-BRSP (Web Services Interoperability) Basic Profile. In contrast to CORBA, DCOM and RMI, the use of SOAP is independent of the way that the applications to be integrated are developed.
Maturity	Both SOAP v1.1 and SOAP v1.2 are now widely adopted in Web Services implementations. Apache Axis2 is a core engine for Web services. It is a complete re-design and re-write of the widely used Apache Axis SOAP stack. Apache Axis2 supports both SOAP v1.1 and SOAP v1.2.
Forward outlook	The W3C XML Protocol Working Group was closed in July 2009. It seems that SOAP v1.1 has no further development ever since SOAP v1.2 became a W3C Recommendation.
Version and rationale for version	In April 2007, SOAP v1.2 (Second Edition) became a W3C Recommendation. WS-BRSP Basic Profile versions 1.2 and 2.0 were finalised in November 2010. SOAP v1.1 and SOAP v1.2 were adopted in WS-BRSP Basic Profile versions 1.2 and 2.0 respectively.
Limitations on the use of this standard	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.

Standard 1b Web Services Description Language (WSDL) v1.1 or WSDL v2.0	
Description	Web Services Description Language (WSDL) v1.1 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. WSDL v2.0 provides a model and an XML format for describing Web services. WSDL v2.0 enables one to separate the description of the abstract functionality offered by a service from concrete details of a service description such as "how" and "where" that functionality is offered. At an abstract level, WSDL v2.0 describes a Web service in terms of the messages it sends and receives. Messages are described independently of a specific wire format using a type system, typically XML Schema. WSDL v2.0 became a W3C Recommendation in June 2007.
Rationale for selection	WSDL is the basis of the work of the Web Services Description Working Group of the W3C's Web Services Activity. WSDL is one of the core technologies which underpins Web Services and has significant industry support from a broad range of infrastructure and application providers. WSDL is included in the WS-BRSP Basic Profile.
Maturity	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. It is widely adopted in Web Services implementations. Apache Axis2 supports the Web Services Description Language, version 1.1 and 2.0, which allows developers to easily build stubs to access remote services, and also to automatically export machine-readable descriptions of deployed services from Apache Axis2.
Forward outlook	W3C has not yet announced further development for WSDL v2.0.
Version and rationale for version	Both version 1.1 and version 2.0 are part of the WS-BRSP Basic Profile and are widely adopted in the market.
Limitations on the use of this standard	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 may arise.

Standard 1c Universal Description, Discovery and Integration (UDDI) v2 or UDDI v3.0.2	
Description	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: • 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

Standard 1c Universal Description, Discovery and Integration (UDDI) v2 or UDDI v3.0.2	
	• Specification pointers – references to specifications and technical information about services • Service types – pointers to technical specifications, such as interface definitions, message formats, message protocols and security protocols. Service interfaces can be described using WSDL and invoked using SOAP. The UDDI business registry can be accessed through both a browser-based interface and programmatically, via SOAP. 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. 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. One of the most significant enhancements of UDDI v3.0.2 is that it allows well-known identifiers for service descriptions to be created, facilitating reuse of service descriptions among registries. This makes it much easier for developers and architects to communicate.
Rationale for selection	UDDI v3.0.2 adds the ability to affiliate registries in keeping with SOA's emphasis on supporting a variety of infrastructural variations and providing a means to define relationships among a variety of UDDI registries. Although from its inception, the specification included concepts such as delegation and distribution among server peers, earlier UDDI definitions relied upon proprietary means of interaction. By contrast, UDDI v3.0.2 provides an open, standardised approach to ensure widely interoperable communication. As indicated by WS-BRSP, UDDI v2 is the sanctioned mechanism for the publication and discovery of Web Services when such function is needed. UDDI has broad industry recognition as a solution to enable the publication and location of services described using WSDL and requested using SOAP.
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 standard on 20 May 2003. UDDI version 3.0.2 was approved as an OASIS standard on 3 February 2005, with its associated registries and directories are now widely used in private and in-house environments. Version 2 of the specification had been adopted by common public repositories and product vendors.
Forward outlook	As Service-Oriented Architecture (SOA) becomes the de facto approach to systems deployment, dynamic discovery services like UDDI v3.0.2 will become increasingly important. As more and more companies begin to deploy private and public registries, products supporting UDDI v3.0.2 will make it easier to bring wide deployment of Web services to market. The enhancements that went into UDDI v3.0.2, such as the support of XML digital signatures for data integrity and authenticity and a pub/sub-mechanism (pub/sub means publish/subscribe of web services) for change notifications, address commonly requested requirements and make it the canonical candidate for enterprise services registries.
Version and rationale for version	Both version 2 and version 3, which has wide product support.

Standard 1c Universal Description, Discovery and Integration (UDDI) v2 or UDDI v3.0.2	
Limitations on the use of this standard	The Web Services that constitute UDDI v2 are not fully conformant with the WS-BRSP 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.

Standard 2 OpenAPI v3.0 or v3.1	
Description	The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to RESTful APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection. When properly defined, a consumer can understand and interact with the remote service with a minimal amount of implementation logic.
Rationale for selection	An OpenAPI definition can then be used by documentation generation tools to display the API, code generation tools to generate servers and clients in various programming languages, testing tools, and many other use cases.
Maturity	Version 3.0 and 3.1 are mature and were released by OpenAPI Initiative in July 2017 and February 2021 respectively..
Forward outlook	Nil
Version and rationale for version	OpenAPI Initiative published patches (v3.0.x) on top of v3.0 from 2017-2020.
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
Common Object Request Broker Architecture (CORBA)	CORBA is an architecture and specification developed through the Object Management Group, sanctioned by ISO, as a standard for distributed objects. CORBA uses the Internet Inter-ORB Protocol (IIOP) for remote request delivery and Interface Definition Language (IDL) for remote service description. 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.

Other Standard(s)	Description
Distributed Component Object Model (DCOM)	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. 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.
Remote Method Invocation (RMI)	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. 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.
WSIL – for locating WSDLs directly from the service provider's site	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. There is no further development on the standard since 2007 and there is no wide adoption observed.

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 v2 AS4-Profile v1.0 WS-Reliability WS-ReliableMessaging WS-Transaction ebXML CPPA	ebMS v2 AS4-Profile v1.0 of ebMS v3	WS-ReliableMessaging WS-Transaction

Remarks:

- AS4-profile of the ebMS 3.0 specification is a lightweight profile based on ebMS 3.0 standard approved as an OASIS standard.
- 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.

Recommended standards

Standard 1 ebXML Message Service (ebMS) v2	
Description	The ebXML Message Service Specification is one of the specifications within the ebXML framework of specifications. 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. This specification is independent of both the payload and the communications protocol used. It utilises W3C's XML Signature standard to provide secure SOAP messaging. ebMS defines an interoperable protocol where any two Message Service implementations can reliably exchange messages sent using once-and-only-once delivery semantics.
Rationale for selection	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.
Maturity	The OASIS ebXML Implementation, Interoperability and Conformance (IIC) Technical Committee (TC) has approved ebMS v2 in May 2003.
Forward outlook	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. Part 2, Advanced Features, complements Core Specification by specifying advanced messaging functionality for message service configuration, message bundling, message across intermediaries (multi-hop) and transfer of (compressed) messages as series of smaller message fragments. Part 2 became an OASIS Committee Specification on 19 May 2011.
Version and rationale for version	Version 2.0, which has been approved by OASIS ebXML Implementation, Interoperability and Conformance (IIC) Technical Committee (TC), is adopted because it is the most widely adopted version.

Standard 1 ebXML Message Service (ebMS) v2	
Limitations on the use of this standard	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.

Standard 2 AS4-Profile v1.0 of ebMS v3	
Description	In 15 February 2013, the OASIS international open standards consortium announced the approval of version 1.0 of the Applicability Statement 4 (AS4) Profile of the ebXML Messaging Services (ebMS) 3.0 standard. It ensures ebXML's continuing relevancy and achieves compatibility with Web services specifications as well as the WS-Security, WS-Reliability, and WS-ReliableMessaging standards.
Rationale for selection	The main benefits of AS4-Profile are compatibility with Web services standards, message pulling capability, and a built-in receipt mechanism. It uses Web Services standards championed by OASIS including the WS-BRSP Basic Profile. It is also a messaging protocol widely adopted in retail and other industries.
Maturity	AS4-Profile is now widely used in the industry and adopted as a standard to exchange messages using web services.
Forward outlook	Cloud Computing is gaining popularity as a computing trend in today's IT environment. There is a growing need for standards that would enable the cloud-based services to interoperate. AS4-Profile is a standard that can achieve such interoperability in the cloud.
Version and rationale for version	Version 1.0 is the current version published by OASIS.
Limitations on the use of this standard	AS4-Profile, is a trimmed down ebMS 3.0 subset of functionalities which is a simplified specification for Web Services B2B messaging based on the just-enough design principles. Although AS4-Profile has been approved as a standard by OASIS, please note that ebMS v3.0 Part 2 (Advanced Features) by itself is yet to be approved as an OASIS standard. Therefore it is recommended to use AS4-Profile as a recommended standard only.

Emerging standards for future consideration

Emerging Standard(s)	Description
WS-ReliableMessaging	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. The latest version is 1.2, released in February 2009.
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. The latest version is 1.2, released in February 2009.

Other candidate standards

Other Standard(s)	Description
WS-Reliability	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 as an OASIS Standard in November 2004. WS-Reliability was considered to be superseded by WS-ReliableMessaging.
ebXML CPPA	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. There was no further update to the standard since 2002.

3.1.2.3 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 virtualisation platforms.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Open Virtualization Format (OVF)	Open Virtualization Format (OVF) v1.1.0	None

Recommended standards

Standard 1 Open Virtualization Format (OVF) v1.1.0	
Description	The Open Virtualization Format (OVF) specification describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines. It is submitted by leading virtualisation companies to the Distributed Management Task Force (DMTF) 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. An OVF package consists of several files, placed in one directory. A one-file alternative is the OVA package, which is a TAR file with the OVF directory inside. An OVF package can describe multiple virtual machines. An OVF package always contains exactly one OVF descriptor (a file with extension .ovf). The OVF descriptor is an XML file which describes the packaged virtual machine; it contains the metadata for the OVF package, such as name, hardware requirements, references to the other files in the OVF package and human-readable descriptions. In addition to the OVF descriptor, the OVF package will typically contain one or more disk images, and optionally certificate files and other auxiliary files.
Rationale for selection	OVF has been the most popular and widely adopted format for portable virtual machine package purpose. The OVF Specification is not tied to any particular virtualisation software or processor architecture.

Standard 1 Open Virtualization Format (OVF) v1.1.0	
Maturity	OVF became a DMTF standard in March 2009 and was broadly supported by virtualisation software such as Oracle VirtualBox, Red Hat Enterprise Virtualization, VMware and XenServer. The OVF standard was approved and published as ISO/IEC 17203:2011 in December 2011, its second edition was published as ISO/IEC 17203:2017 in September 2017.
Forward outlook	OVF 2.0 released in January 2013 brings an enhanced set of capabilities to the packaging of virtual machines, making the standard applicable to a broader range of cloud use cases that are emerging as the industry enters the cloud era. The latest version is OVF 2.1.1 which was released in August 2015.
Version and rationale for version	Version 1.1.0 released in January 2010 was the mature version supported by vendors. For the latest version OVF 2.1.1, it will take time for vendors to include its support in their future products.
Limitations on the use of this standard	OVF is not a specification that describes a virtual disk. To import OVF content requires hypervisor compatibility with the associated virtual disk.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.1.2.4 Application interface for content management systems and repositories

Justification for inclusion and usage

Define the interface standards for cross content management systems and repositories data sharing in G2G collaboration.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Content Management Interoperability Services (CMIS)	Content Management Interoperability Services (CMIS) v1.1	None

Recommended standards

Standard 1 Content Management Interoperability Services (CMIS) v1.1	
Description	Content Management Interoperability Services (CMIS) is an open standard for improving interoperability between content management systems and repositories. CMIS defines an abstraction layer for controlling diverse content management systems and repositories using Web protocols. A domain model and three protocol bindings including Restful AtomPub binding (RFC 5023), Web Services binding (WSDL) and browser binding (Java Script Object

Standard 1 Content Management Interoperability Services (CMIS) v1.1	
	Notation, JSON, RFC 4627) are defined for applications to communicate with content management systems and repositories in a vendor-neutral format. CMIS provides an interface for an application to access a repository, or for a repository to access other repositories. It defines a core data model which enumerates the persistent information entities ("objects") that are managed by the repository. It specifies a generic and universal set of capabilities of content management systems and a set of services for working with those capabilities to access and manipulate the objects. Many open source and commercial CMIS server stores, client applications and program libraries (such as Microsoft SharePoint 2013, IBM FileNet Content Manager and its enterprise class client platform – IBM Content Navigator, EMC Documentum, Alfresco, and Drupal) have claimed support on CMIS.
Rationale for selection	CMIS is an open standard widely used in the industry. It is backed by leading vendors and is adopted by most of the commonly used content management systems and repositories. Market acceptance of CMIS is ensured. Some organisations even started to place CMIS into their ECM strategies and make it part of their architecture plans. Both versions of CMIS (v1.0 & v1.1) were approved to be official OASIS standards, a status which signifies the highest level of ratification. Governments in other countries are also adopting CMIS. For example, CMIS is included in the Enterprise Content Management Strategy of the British Columbia Government. Government of Alberta also adopted CMIS as its Information Management and Technology (IMT) standard. There are many successful stories demonstrating interoperable CMIS solutions across different platforms. A recently published research report by Forrester Research found that organisations were using CMIS to great benefit, including a U.S. Department of Defense agency using CMIS to migrate their content out of their legacy system to newer platforms, and SAP using CMIS to create a mobile application to collect content from 15 content sources including Alfresco, OpenText, SAP Knowledge Management and SharePoint.
Maturity	CMIS v1.0 was approved as an OASIS standard on 1 May 2010. The latest version 1.1 was approved as an OASIS standard on 23 May 2013.
Forward outlook	Nil
Version and rationale for version	Version 1.1 was chosen because it has more features and better interoperability than version 1.0.
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	

3.1.2.5 Asynchronous message exchange between application systems

Justification for inclusion and usage

Defines specifications for applications to exchange messages asynchronously to facilitate the development and integration of applications handling large number of devices, which will be increasingly adopted in the Government.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Advanced Message Queuing Protocol (AMQP) Constrained Application Protocol (CoAP) Message Queue Telemetry Transport (MQTT)	Advanced Message Queuing Protocol (AMQP) v1.0 Message Queue Telemetry Transport (MQTT) v3.1.1	Constrained Application Protocol (CoAP) Message Queue Telemetry Transport (MQTT) v5.0 Data Distribution Service (DDS)

Recommended standards

Standard 1 Advanced Message Queuing Protocol (AMQP) v1.0	
Description	AMQP is an open standard for passing business messages between applications or organisations. It connects systems, feeds business processes with the information they need and reliably transmits onward the instructions that achieve their goals. AMQP is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns. It provides flow controlled, message-oriented communication with message-delivery guarantees such as at-most-once (where each message is delivered once or never), at-least-once (where each message is certain to be delivered, but may do so multiple times) and exactly-once (where the message will always certainly arrive and do so only once), and authentication and/or encryption based on SASL and/or TLS. It assumes an underlying reliable transport layer protocol such as Transmission Control Protocol (TCP).
Rationale for selection	AMQP provides an efficient, secure, robust means to connect disparate systems and organisations in a standard way. It is an open and mature standard which avoids vendor lock-in and is easy for adoption in different application systems.
Maturity	AMQP version 1.0 specification was approved by OASIS in October 2012. AMQP version 1.0 was approved for release by ISO/IEC in April 2014 and given the designation 'ISO/IEC 19464'. AMQP is supported by companies including Bank of America, N.A., Deutsche Börse Group, IIT Software GmbH, INETCO Systems Ltd, JPMorgan Chase Bank & Co., Kaazing Corporation, Microsoft Corporation, my-Channels, Progress Software, Red Hat Inc., Software AG, Solace Systems Inc., StormMQ, VMware Inc. These companies are also members of the OASIS AMQP Member Section. There are commercial and open source implementations of the AMQP available on the market. For example: Apache Qpid, RabbitMQ, Solace Message Router and StormMQ.
Forward outlook	Nil.

Standard 1 Advanced Message Queuing Protocol (AMQP) v1.0	
Version and rationale for version	Version 1.0, which has been approved for release by ISO/IEC in April 2014 and was given the designation 'ISO/IEC 19464'.
Limitations on the use of this standard	None.

Standard 2 Message Queuing Telemetry Transport (MQTT) v3.1.1	
Description	MQTT is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium. The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections. Its features include: - Use of the publish/subscribe message pattern which provides one-to-many message distribution and decoupling of applications. - A messaging transport that is agnostic to the content of the payload. - Three qualities of service for message delivery: ■ "At most once", where messages are delivered according to the best efforts of the operating environment. Message loss can occur. This level could be used, for example, with ambient sensor data where it does not matter if an individual reading is lost as the next one will be published soon after. ■ "At least once", where messages are assured to arrive but duplicates can occur. ■ "Exactly once", where message are assured to arrive exactly once. This level could be used, for example, with billing systems where duplicate or lost messages could lead to incorrect charges being applied. - A small transport overhead and protocol exchanges are minimised to reduce network traffic. - There is a mechanism to notify interested parties when an abnormal disconnection occurs.
Rationale for selection	MQTT defines an extremely lightweight publish/subscribe messaging transport protocol. Because it requires significantly less bandwidth and is easy to implement, MQTT is well suited for IoT applications where resources such as battery power and bandwidth are at a premium.
Maturity	MQTT version 3.1.1 specification was approved by OASIS in 2014. MQTT version 3.1.1 was approved for release by ISO/IEC in June 2016 and given the designation 'ISO/IEC 20922'. MQTT is backed by major players in the industry. MQTT is supported by major public cloud IoT platform providers including AWS IoT, IBM Watson IoT Platform and Microsoft Azure IoT Hub. There are commercial and open source implementations of the MQTT protocol available on the market. For example: Apache ActiveMQ, Eclipse Paho, Emitter, HiveMQ, IBM Websphere, Mosquitto, MQ Telemetry, RabbitMQ and Solace Message Router.
Forward outlook	The range of MQTT applications continues to grow. In the healthcare sector, practitioners use the protocol to communicate with bio-medical devices such as blood pressure monitors. Oil and gas companies use MQTT to monitor thousands of miles of pipelines. MQTT is emerging as a fundamental enabler for telematics, infotainment, and other connected vehicle applications. MQTT is also becoming increasingly popular for interactive mobile applications.

Standard 2 Message Queuing Telemetry Transport (MQTT) v3.1.1	
Version and rationale for version	Version 3.1.1, which was approved for release by ISO/IEC in June 2016 and given the designation 'ISO/IEC 20922'.
Limitations on the use of this standard	Encryption is not natively supported by the protocol. Encryption across the network can be handled with SSL, independently of the MQTT protocol itself. Additional security can be added by an application encrypting data that it sends and receives, but this is not something built-in to the protocol.

Emerging standards for future consideration

Emerging Standard(s)	Description
Constrained Application Protocol (CoAP)	CoAP is a specialised web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things (IoT). The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation. It is also a specialised Internet Application Protocol for constrained devices that enables those constrained devices called "nodes" to communicate with the wider Internet using similar protocols. CoAP is designed for use between devices on the same constrained network (e.g., low-power, lossy networks), between devices and general nodes on the Internet, and between devices on different constrained networks both joined by an Internet. CoAP is also being used via other mechanisms, such as SMS on mobile communication networks.
Message Queue Telemetry Transport (MQTT) v5.0	MQTT is a message protocol designed for constrained devices with low bandwidth. It is one of the most commonly used protocols for Internet of Things ("IoT") projects. On 7 March 2019, the Organization for the Advancement of Structured Information Standards ("OASIS") published the official MQTT version 5.0 with significant updates (which supersedes the existing version 3.1.1). However, the maturity and adoption by the industry has yet to be confirmed.
Data Distribution Service (DDS)	DDS is a machine-to-machine ("M2M") protocol and Application Programming Interface ("API") standard for data-centric connectivity. The protocol is designed for large-scale business and mission-critical Internet of Things ("IoT") applications. DDS supports decentralised architecture and transparently addresses peer-to-peer, device-to-device, device-to-cloud and cloud-to-cloud communication. This eliminates bottleneck and single point of failure. With respect to security, a comprehensive security model has been defined for compliant DDS implementations. This provides standardised authentication, encryption, access control and logging capabilities to enable secure data connectivity. DDS version 1.4 was published by the Object Management Group in 2015. Besides, other related standards and extensions were also defined to support the implementation of DDS, including DDS-Security v1.1, DDS-RTPS v2.3, DDS-XML v1.0, .etc. DDS is currently not supported by the major cloud service providers, such as Amazon Web Services ("AWS"), Microsoft Azure and Google Cloud. Since cloud-based platforms are key components for connecting IoT devices, it is recommended to include DDS as an emerging standard and keep in view its adoption in the cloud services industry.

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	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. ebXML RegRep v4.0 released in January 2012, which is a single multi-part standard consisting of Part 1: ebRIM (ebXML Registry Information Model) is the latest OASIS approved standard. While the ebXML RIM forms part of the ISO 15000 standard, OASIS technical committees retain the responsibility for maintaining and advancing ebXML standards.

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	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. ebXML RegRep v4.0 released in January 2012, which is a single multi-part standard consisting of Part 2: ebXML RS, is the latest OASIS approved standard.

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	Web Services Addressing v1.0 - Core (WS-Addressing) defines two constructs, message addressing properties and endpoint references, that normalise the information typically provided by transport protocols and messaging systems in a way that is independent of any particular transport or messaging system. A Web service endpoint is an entity, processor, or resource to which Web service messages can be addressed. Endpoint references convey the information needed to address a Web service endpoint. 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. Web Services Addressing v1.0 is a W3C recommendation. The Web Services Addressing Working Group completed its deliverables and closed in September 2007.

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	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. 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. The specifications became W3C Recommendations in September 2007.

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 modelled 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 Model and 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 Model and Notation (BPMN), etc. BMM is a framework to facilitate development and management of business plans. It supports processes that are driven by business change. BMM v1.3 was published in May 2015. BPDM is a standard to present business process models. BPDM v1.0 was published in November 2008. BPMM defines framework to manage business process improvements and maturity levels. BPMM v1.0 was published in June 2008. BPMN defines standardised notations for business process design and process implementation so that it can be understandable by all business users including the business analysts that create the initial drafts of the processes, the technical developers that implement processes, and the business people that manage and monitor the processes. BPMN v2.0.1 became ISO/IEC 19510:2013 in July 2013. Object Management Group (OMG) released BPMN v2.0.2 in January 2014, but the ISO/IEC 19510:2013 standard has not been updated.
Web Services Business Process Execution Language (WS-BPEL)	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 standardisation 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. 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. 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. WS-BPEL v2.0 became an OASIS standard in April 2007.

Standard(s)	Description
Business Process Specification Schema (BPSS)	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. 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. The ebXML BPSS (ebBP) v2.0.4 became an OASIS standard in December 2006. This version of the ebBP technical specification addresses Business Collaborations between any number of parties (Business Collaborations specialised 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 organisations.

Other candidate standards

Other Standard(s)	Description
Web Services Choreography	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 has been a W3C Candidate Recommendation since November 2005. The W3C Web Services Choreography Working Group was closed in July 2009, and there has been no further development of this standard since then.

3.1.4.2 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)	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. 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. SML 1.1 became a W3C Recommendation in May 2009.

3.1.4.3 Cloud management interface

Justification for inclusion and usage

Defines common interfaces to request, deploy, administer, and use cloud infrastructure services.

Analysis

The Distributed Management Task Force (DMTF) is developing a common API for cloud management as standard interface to facilitate easy switching between the cloud infrastructure provisions by service consumers. The focus of work is on standardising interactions between cloud environments by developing specifications that deliver architectural semantics and implementation details to achieve interoperable cloud management between service providers and their consumers and developers.

Standards for future consideration

Standard(s)	Description
Open Cloud Computing Interface (OCCI)	OCCI was originally initiated to create a remote management API for IaaS model-based services, allowing for the development of interoperable tools for common tasks including deployment, autonomic scaling and monitoring. It has since evolved into a flexible API with a strong focus on interoperability while still offering a high degree of extensibility. The current release of the OCCI is suitable to serve many other models in addition to IaaS, including PaaS and SaaS. The first version v1.1 was published in April 2011 and the latest version v1.2 was published in February 2016. The OCCI Core and Infrastructure specification documents have been published as Proposed Recommendations under the Open Grid Forum (OGF). Some open source cloud computing tools such as OpenNebula, OpenStack and Apache CloudStack are supporting OCCI. One example of the OCCI adoption is the Italian National Institute of Nuclear Physics (INFN)'s use of OCCI APIs as the interface of their WNoDoes application. However, other major commercial cloud providers do not support OCCI at the moment.
Cloud Infrastructure Management Interface (CIMI)	CIMI is a specification created by the Cloud Management Working Group (CMWG) of the Distributed Management Task Force (DMTF). CIMI is an open standard IaaS management interface and it provides a self-service interface for IaaS allowing users to dynamically provide, configure and administer the cloud usage. The latest version CIMI v2.0.0 was released in August 2016. CIMI v1.1.0 became ISO Standard ISO/IEC 19831:2015 in April 2015. Being the first cloud standard from CMWG and a rather new standard, CIMI is gaining industry support.

3.1.4.4 Cloud data management interface

Justification for inclusion and usage

Defines the functional interface that applications will use to create, retrieve, update and delete data elements from the cloud.

Analysis

As part of this interface the client will be able to discover the capabilities of the cloud storage offering and use this interface to manage containers and the data that is placed in them. In addition, metadata can be set on containers and their contained data elements through this interface.

CDMI is used by administrative and management applications to manage containers, accounts, security access and monitoring/billing information, even for storage that is accessible by other protocols. The capabilities of the underlying storage and data services are exposed so that clients can understand the offering.

Standards for future consideration

Standard(s)	Description
Cloud Data Management Interface (CDMI)	CDMI specifies the interface to access cloud storage and to manage the data stored therein. The standard is applicable to developers who are implementing or using cloud storage. The latest version CDMI v1.1.1 was released as a Storage Networking Industry Association (SNIA) Technical Position in March 2015 and published as ISO/IEC 17826:2016 in July 2016.

3.1.4.5 Web application interface for data access and publishing

Justification for inclusion and usage

Defines a Web protocol for Web applications to perform CRUD-style access (Create, Read, Update and Delete) and publish data on the Web.

Analysis

Traditionally, protocols such as ODBC and JDBC provides an application interface for CRUD-style operations against backend databases. Web-based equivalent protocols against data sources on the Web have been developed and open standards are emerging. Such protocols enables information to be accessed from a variety of sources including but not limited to relational databases, file systems, content management systems, and traditional websites.

Standards for future consideration

Standard(s)	Description
Open Data Protocol (OData)	OData defines an abstract data model and a protocol that let any client access information exposed by any data source. It enables information to be accessed from a variety of sources including (but not limited to) relational databases, file systems, content management systems, and traditional websites and simplifies data sharing in a uniform way across disparate applications in enterprise, Cloud, and mobile devices. OData version 4.0 became an OASIS standard in February 2014. In recent years OData is also available on non-Microsoft platforms such as iOS and Android. The OData 4.0 Core Protocol is available as ISO/IEC 20802-1:2016, and the OData 4.0 JSON Format is available as ISO/IEC 20802-2:2016. As of 30 January 2018, "OData 4.01 Part 1: Protocol" had been published by OASIS as a committee specification. Open Data Protocol (OData) Version 4.01 was approved as an OASIS Standard on 18 June 2020 with enhancements including: • Simplified syntax and payloads • Extended query patterns • Enhanced update capabilities • New JSON Metadata and Batch Formats While OData version 4.01 has been approved as an OASIS standard, its adoption by the industry is yet to be seen.

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.		

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. XHTML (eXtensible Hypertext Markup Language) is a family of eXtensible Markup Language (XML) and W3C describes XHTML as "a reformulation of HTML as an application of the XML." XHTML 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. HTML (v4.01) was recommended by W3C in December 1999 while XHTML (v1.0) was recommended by W3C in January 2000. The latest version of HTML5. 2 was published as a recommended standard by W3C on 14 December 2017, while XHTML5 was published in October 2014.
Forward outlook	In October 2014, W3C has published HTML5, together with XHTML5, as the recommended standards. HTML5.2 was released on 14 December 2017. W3C continues the work on HTML 5.3 specifications and the editor's draft was published on 18 October 2018.
Version and rationale for version	HTML and XHTML implemented by commonly adopted versions of browsers. HTML5.2 and XHTML5 are the latest recommended standards approved by W3C in December 2017 and October 2014 respectively. 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/index.html).

Standard 1 HTML and XHTML implemented by commonly adopted versions of browsers	
Limitations on the use of this standard	Support of major browsers on HTML5/5.1/5.2 varies. It is strongly recommended that content authors test compatibility of their content against the prevailing versions of popular browsers and consult the appropriate vendor documentation which discusses restrictions and deviations from the specifications. 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. Web masters should also state on their Web page how the content can best be viewed.

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 Edition 5.1	None

Recommended standards

Standard 1 ECMA 262 Script Edition 5.1	
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 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.

Standard 1 ECMA 262 Script Edition 5.1	
Maturity	The development of this standard started in November 1996. The first edition of this ECMA standard was adopted by the ECMA General Assembly in June 1997. The 3rd Edition of ECMA-262 was adopted by the ECMA General Assembly in December 1999 and published as ISO/IEC 16262:2002 in June 2002. Edition 5.1 of the ECMA 262 standard was released in June 2011 and was fully aligned with the third edition of the international standard ISO/IEC 16262:2011. ISO/IEC 16262:2011 was withdrawn and revised by ISO/IEC 22275:2018 in May 2018.
Forward outlook	ECMA 262 standard will continue to be developed by ECMA International. It is a vibrant language and the evolution of the language is not yet complete. Significant technical enhancement will continue with future editions of this specification. Starting from ECMAScript 2016, new version of the ECMAScript will be released yearly. The latest version is 11th Edition, which was released in June 2020.
Version and rationale for version	Edition 5.1 is the version that is supported by the popular browsers. With the exception of Microsoft Internet Explorer version 11 (IE11), support of most desktop browsers on ECMAScript 2015 (6th Edition) is mature. For later editions, the support by major browsers vary, and notably the support by IE11 is very limited.
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 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 implemented by commonly adopted versions of browsers PDF	None
Remarks: 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. The PDF content providers should indicate which viewer software the recipients can use and supply a link to the viewer software if necessary.		

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 32000-1 in July 2008. PDF 2.0 (ISO 32000-2:2017) was published by the ISO in July 2017 and is revised by ISO 32000-2:2020 in December 2020.
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.
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	

3.2.1.4 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 .rtf HTML PDF .doc .odt .docx .ppt .odp .pptx .xls .ods .xlsx PDF/A	.txt .rtf v1.6 HTML PDF v1.2, 1.3, 1.4, 1.5, 1.6, 1.7 (ISO 32000-1) or 2.0 (ISO 32000-2:2020) .doc (Word 97 file format which is used by Word 97 and later versions) .odt .docx (ISO/IEC 29500-1) .ppt (PowerPoint 97 file format which is used by PowerPoint 97 and later versions) .odp .pptx (ISO/IEC 29500-1) .xls (Excel 97 file format which is used by Excel 97 and later versions) .ods .xlsx (ISO/IEC 29500-1) PDF/A-1a (ISO 19005-1 Level A) PDF/A-1b (ISO 19005-1 Level B)	None
Remarks: For HTML file types, members of the public should use features of HTML v4.01 that are implemented in common by the prevailing versions of popular browsers.		

Recommended standards

Standard 1 .txt	
Description	Plain/unformatted text files.
Rationale for selection	*De facto* standard for plain/unformatted text extensively supported by word processing packages, publishing tools, content management applications, e-mail applications etc.
Maturity	Mature.
Forward outlook	Will continue to be supported as a common format.

Standard 1 .txt	
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 *de facto* 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, 1.7 (ISO 32000-1) or 2.0 (ISO 32000-2:2020)
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, 1.7 (ISO 32000-1) or 2.0 (ISO 32000-2:2020)	
Version and rationale for version	PDF versions are explicitly specified in order to ascertain 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. The old versions of PDF are still acceptable in order to avoid forcing members of the public to upgrade their PDF generation software.

Standard 5 .doc (Word 97 file format which is used by Word 97 and later versions)
Please refer to the area "Formatted document file type for collaborative editing" for details on .doc

Standard 6 .odt
Please refer to the area "Formatted document file type for collaborative editing" for details on .odt

Standard 7 .docx (ISO/IEC 29500-1)
Please refer to the area "Formatted document file type for collaborative editing" for details on .docx

Standard 8 .ppt (PowerPoint 97 file format which is used by PowerPoint 97 and later versions)
Please refer to the area "Presentation file type for collaborative editing" for details on .ppt

Standard 9 .odp
Please refer to the area "Presentation file type for collaborative editing" for details on .odp

Standard 10 .pptx (ISO/IEC 29500-1)
Please refer to the area "Presentation file type for collaborative editing" for details on .pptx

Standard 11 .xls (Excel 97 file format which is used by Excel 97 and later versions)
Please refer to the area "Spreadsheet file type for collaborative editing" for details on .xls

Standard 12 .ods
Please refer to the area "Spreadsheet file type for collaborative editing" for details on .ods

Standard 13 .xlsx (ISO/IEC 29500-1)
Please refer to the area "Spreadsheet file type for collaborative editing" for details on .xlsx

Standard 14 PDF/A-1a (ISO 19005-1 Level A)	
Description	PDF/A-1 (ISO 19005-1:2005) is a constrained form of Adobe PDF version 1.4 intended to be suitable for long-term preservation of page-oriented documents for which PDF is already being used in practice. PDF/A-1a indicates complete compliance with the ISO 19005-1 requirements, including those related to structural and semantic properties of documents.
Rationale for selection	It is recognised by ISO and widely adopted by different governments and commercial entities over the world.
Maturity	Approved since 2005.

Standard 14 PDF/A-1a (ISO 19005-1 Level A)	
Forward outlook	PDF/A-2 and PDF/A-3 which are constrained forms of Adobe PDF version 1.7 were published in 2011 and 2012 respectively. PDF/A-2 and PDF/A-3 address some of the new features with versions 1.5, 1.6 and 1.7 of PDF standard. PDF/A-2 and PDF/A-3 will not necessarily conform to PDF/A-1 and vice versa.
Version and rationale for version	PDF/A-1a. PDF/A-1a requires tagging for structure as well as Unicode character maps for fonts. The objective for PDF/A-1a includes the goals for PDF/A-1b and accessibility for physically impaired users. The tags for accessibility enable screen readers to provide some form of description for images. Since the standard was published in 2005, tools for creation, conversion, and validation have been reaching the market steadily.
Limitations on the use of this standard	None.

Standard 15 PDF/A-1b (ISO 19005-1 Level B)	
Description	PDF/A-1 (ISO 19005-1:2005) is a constrained form of Adobe PDF version 1.4 intended to be suitable for long-term preservation of page-oriented documents for which PDF is already being used in practice. PDF/A-1b indicates minimal compliance to ensure that the rendered visual appearance of a conforming file is preservable over the long term.
Rationale for selection	It is recognised by ISO and widely adopted by different governments and commercial entities over the world.
Maturity	Approved since 2005.
Forward outlook	PDF/A-2 and PDF/A-3 which are constrained forms of Adobe PDF version 1.7 were published in 2011 and 2012 respectively. PDF/A-2 and PDF/A-3 address some of the new features with versions 1.5, 1.6 and 1.7 of PDF standard. PDF/A-2 and PDF/A-3 will not necessarily conform to PDF/A-1 and vice versa.
Version and rationale for version	PDF/A-1b. PDF/A-1b variant is for content that has no accessibility tagging. It is useful for scanned documents. The objective for PDF/A-1b is to ensure reliable reproduction of the visual appearance of the document. Since the standard was published in 2005, tools for creation, conversion, and validation have been reaching the market steadily.
Limitations on the use of this standard	PDF/A-1b indicates minimal compliance for the reliable reproduction of a document's visual appearance. Document's accessibility such as language specification, hierarchical document structure, character mappings to Unicode and tagged text spans and descriptive text for images and symbols are not included.

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 long term preservation

Justification for inclusion and usage

Required to support long term preservation of record/document.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
PDF/A	PDF/A-1a (ISO 19005-1 Level A) PDF/A-1b (ISO 19005-1 Level B)	None
Remarks: Documents are created in or converted to PDF/A file type/format, for long term preservation to ensure that they can still be accessed in the future.		

Recommended standards

Standard 1 PDF/A-1a (ISO 19005-1 Level A)
Please refer to the area "Document file type for receiving documents under ETO" for details on PDF/A-1a (ISO 19005-1 Level A)

Standard 2 PDF/A-1b (ISO 19005-1 Level B)
Please refer to the area "Document file type for receiving documents under ETO" for details on PDF/A-1b (ISO 19005-1 Level B)

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.6 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 .docx	.rtf v1.6 HTML and XHTML implemented by commonly adopted versions of browsers .doc (Word 97 file format which is used by Word 97 and later versions) .odt .docx (ISO/IEC 29500-1)	

Remarks:

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 belongs to the same family, then tool-specific format like .sxw may be used for file exchange.

For HTML documents, the sender is also recommended to test their content against the prevailing versions of popular browsers.

B/Ds should refer to the then 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.

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.

Standard 3 .doc (Word 97 file format which is used by Word 97 and later versions)	
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://technet.microsoft.com/en-us/library/cc178953.aspx

Standard 4 .odt	
Description	The .odt format is the default document format for OpenOffice.org v2.0 or later. It is a document format introduced in the OpenOffice.org v2.0. It is based on the OpenDocument ratified by the OASIS, but it uses its own specific file extension. OpenDocument is made up of a single XML schema for text, spreadsheet and presentation 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.
Rationale for selection	The .odt format is expected to be compatible with other document formats which conform to the prevailing version of OpenDocument. 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 later or its variants. 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 or later and also other OpenOffice variants.
Maturity	Mature for adoption. It is observed that OpenDocument file format has been well received by the user community.
Forward outlook	.odt is envisaged to gain extensive use among the users of OpenOffice.org or its variants.
Version and rationale for version	OpenDocument 1.0 was published by OASIS in May 2005 and adopted by ISO as ISO/IEC 26300:2006 in December 2006. OpenDocument 1.1 was published by OASIS in February 2007 and adopted by ISO as ISO/IEC 26300:2006/Amd 1:2012 in March 2012. OpenDocument 1.2 was published by OASIS in September 2011 and adopted by ISO as ISO/IEC 26300-1:2015 in July 2015.
Limitations on the use of this standard	None.

Standard 5 .docx (ISO/IEC 29500-1)	
Description	The ".docx" file extension represents document files created by office applications using the ISO/IEC 29500-1 format.
Rationale for selection	The Office Open XML-based word processing format using .docx as a file extension has been the default format produced for new documents by versions of Microsoft Word since Word 2007 and supported by a wide variety of similar word-processing applications in the market.

Standard 5 .docx (ISO/IEC 29500-1)	
Maturity	Mature for adoption. ISO/IEC 29500-1:2008 was published in November 2008. ISO/IEC 29500-1:2011 was published in August 2011. ISO/IEC 29500-1:2012 was published in September 2012. ISO/IEC 29500-1:2016 was published in November 2016.
Forward outlook	ISO/IEC 29500-1 family is likely to remain one of the major document file formats in the near future.
Version and rationale for version	Any version of DOCX can be used in this area. The content providers should indicate which editor/viewer software the recipients can use and supply a link to such software if necessary.
Limitations on the use of this standard	Users of Microsoft Word 2007 or earlier versions may encounter compatibility issues on processing files created in this new format.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.7 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 .pptx	.ppt (PowerPoint 97 file format which is used by PowerPoint 97 and later versions) .odp .pptx (ISO/IEC 29500-1)	

Remarks:
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 belongs to the same family, then tool-specific format like .sxi may be used for file exchange. B/Ds should refer to the then 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.

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.
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://technet.microsoft.com/en-us/library/cc178953.aspx

Standard 2 .odp	
Description	The .odp format is the default presentation format for OpenOffice.org v2.0 or later. It is a presentation format introduced in the OpenOffice.org v2.0. It is based on the OpenDocument ratified by the OASIS, but it uses its own specific file extension. OpenDocument is made up of a single XML schema for text, spreadsheet and presentation 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 2 .odp	
Rationale for selection	The .odp format is expected to be compatible with other document formats which conform to the prevailing version of OpenDocument. 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 later or its variants. 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 .odp format is the default file format in the open-source office suite OpenOffice.org v2.0 or later.
Maturity	It is observed that OpenDocument file format 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	OpenDocument 1.0 was published by OASIS in May 2005 and adopted by ISO as ISO/IEC 26300:2006 in December 2006. OpenDocument 1.1 was published by OASIS in February 2007 and adopted by ISO as ISO/IEC 26300:2006/Amd 1:2012 in March 2012. OpenDocument 1.2 was published by OASIS in September 2011 and adopted by ISO as ISO/IEC 26300-1:2015 in July 2015.
Limitations on the use of this standard	None.

Standard 3 .pptx (ISO/IEC 29500-1)	
Description	The ".pptx" file extension represents presentation files created by office applications using the ISO/IEC 29500-1 format.
Rationale for selection	The Office Open XML-based presentation format using .pptx as a file extension has been the default format produced for new documents by versions of Microsoft PowerPoint since PowerPoint 2007 and supported by a wide variety of similar presentation applications in the market.
Maturity	Mature for adoption. ISO/IEC 29500-1:2008 was published in November 2008. ISO/IEC 29500-1:2011 was published in August 2011. ISO/IEC 29500-1:2012 was published in September 2012. ISO/IEC 29500-1:2016 was published in November 2016.
Forward outlook	ISO/IEC 29500-1 family is likely to remain one of the major presentation file formats in the near future.
Version and rationale for version	Any version of PPTX can be used in this area. The content providers should indicate which editor/viewer software the recipients can use and supply a link to such software if necessary.
Limitations on the use of this standard	Users of Microsoft PowerPoint 2007 or earlier versions may encounter compatibility issues on processing files created in this new format.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.8 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 .xlsx .ods CSV	.xls (Excel 97 file format which is used by Excel 97 and later versions) .xlsx (ISO/IEC 29500-1) .ods Comma-Separated Values (CSV) text file	

Remarks:

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 belongs to the same family, then tool-specific format like .sxc may be used for file exchange.

B/Ds should refer to the then 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.

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.

Standard 1 .xls (Excel 97 file format which is used by Excel 97 and later versions)	
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://technet.microsoft.com/en-us/library/cc178953.aspx

Standard 2 .xlsx (ISO/IEC 29500-1)	
Description	The ".xlsx" file extension represents spreadsheet files created by office applications using the ISO/IEC 29500-1 format.
Rationale for selection	The Office Open XML-based spreadsheet format using .xlsx as a file extension has been the default format produced for new documents by versions of Microsoft Excel since Excel 2007 and supported by a wide variety of similar spreadsheet applications in the market.
Maturity	Mature for adoption. ISO/IEC 29500-1:2008 was published in November 2008. ISO/IEC 29500-1:2011 was published in August 2011. ISO/IEC 29500-1:2012 was published in September 2012. ISO/IEC 29500-1:2016 was published in November 2016.
Forward outlook	ISO/IEC 29500-1 family is likely to remain one of the major spreadsheet file formats in the near future.
Version and rationale for version	Any version of XLSX can be used in this area. The content providers should indicate which editor/viewer software the recipients can use and supply a link to such software if necessary.
Limitations on the use of this standard	Users of Microsoft Excel 2007 or earlier versions may encounter compatibility issues on processing files created in this new format.

Standard 3 .ods	
Description	The .ods format is the default spreadsheet format for OpenOffice.org v2.0 or later. It is a spreadsheet format introduced in the OpenOffice.org v2.0. It is based on the OpenDocument ratified by the OASIS, but it uses its own specific file extension. OpenDocument is made up of a single XML schema for text, spreadsheet and presentation 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 3 .ods	
Rationale for selection	The .ods format is expected to be compatible with other document formats which conform to the prevailing version of OpenDocument. 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 later or its variants. 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 .ods format is the default file format in the open-source office suite OpenOffice.org v2.0 or later and also other OpenOffice variants.
Maturity	Mature for adoption. It is observed that OpenDocument file format 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	OpenDocument 1.0 was published by OASIS in May 2005 and adopted by ISO as ISO/IEC 26300:2006 in December 2006. OpenDocument 1.1 was published by OASIS in February 2007 and adopted by ISO as ISO/IEC 26300:2006/Amd 1:2012 in March 2012. OpenDocument 1.2 was published by OASIS in September 2011 and adopted by ISO as ISO/IEC 26300-1:2015 in July 2015.
Limitations on the use of this standard	None.

Standard 4 Comma-Separated Values (CSV) text file	
Description	A comma-separated values (CSV) file stores tabular data (numbers and text) in plain text. Each line of the file is a data record. Each record consists of one or more fields, separated by commas.
Rationale for selection	Common standard for tabular data in text is extensively supported by spreadsheet processing packages.
Maturity	Mature. IETF RFC 4180 was published for information purpose in October 2005 and was updated by RFC 7111 in January 2014.
Forward outlook	Will continue to be supported as a common format.
Version and rationale for version	Not applicable, there is only one version of CSV format.
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	

3.2.1.9 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.

Standard 1 .jpg	
Forward outlook	JPEG 2000 is a new image coding system that is suitable for a wide range of uses from portable digital cameras to advanced pre-press, medical imaging and other key sectors. JPEG 2000 has 12 parts, with Part 10 remaining uncompleted and Part 7 withdrawn. Part 1, Core coding system (completed) Part 2, Extensions (completed) Part 3, Motion JPEG 2000 (completed) Part 4, Conformance (completed) Part 5, Reference software (completed) Part 6, Compound image file format (completed) Part 7, abandoned Part 8, JPSEC (completed) Part 9, JPIP (completed) Part 10, JP3D (Working Draft) Part 11, JPWL (wireless) (completed) Part 12, ISO Base Media File Format (completed)
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 *de facto* 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.
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 *de facto* standard of particular benefit for images that will not tolerate information loss.
Maturity	Mature. Version 6 was published in 1992.

Standard 3 .tif v6	
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.
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.

3.2.1.10 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 10646 and HKSCS	ISO/IEC 10646:2003 with Amendment 1 and HKSCS-2004 – for encoding content in English or Chinese (Chinese characters are restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO/IEC 10646 standard and the HKSCS-2004) ISO/IEC 10646:2011 – for encoding content in English or Chinese (Chinese characters are restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO/IEC 10646 standard)	None

Remarks:

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

ISO/IEC 10646 is the standard for the common Chinese language interface. Unicode (ISO/IEC 10646 or UTF-8) shall be adopted for newly established Chinese version websites or websites undergoing major revamp. For details, please refer to "Technical Notes on Website Development and Maintenance", which is available at:

https://www.digitalpolicy.gov.hk/en/our_work/community/web_mobileapp_accessibility/doc/technical_notes.pdf

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

https://www.ccli.gov.hk/en/iso10646/iicore.html.

Recommended standards

Standard 1 ISO/IEC 10646:2003 with Amendment 1	
Description	The ISO/IEC 10646:2003, published in 2003, is a single publication as the result of the merger of the previous two releases of ISO/IEC 10646 standards: 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. All HKSCS-2004 characters are included in the ISO/IEC 10646:2003 with Amendment 1.
Rationale for selection	ISO/IEC 10646 is widely supported by a broad range of products, including databases, fonts, printing tools, internationalisation libraries and office productivity tools.
Maturity	The ISO/IEC 10646:2003 was published in 2003 and its Amendment 1 was published in 2005. Adoption of platforms supporting these standards in the community seems rapidly increasing. Software and conversion module handling the compatibility of ISO/IEC 10646-1:2000/HKSCS and ISO/IEC 10646:2003 are available.
Forward outlook	Please refer to the Forward outlook of the Standard 3 ISO/IEC 10646:2011.
Version and rationale for version	Products supporting ISO/IEC 10646 are mature. The addition of ISO/IEC 10646:2003 would enable the interoperability of B/Ds' systems using up-to-date universal character set based on ISO/IEC 10646.
Limitations on the use of this standard	Existing application designed for ISO/IEC 10646-1:2000 shall be enhanced to handle those newly included Chinese characters in the ISO/IEC 10646:2003, most of them require more internal storage per character. The migration of IT systems with characters assigned in Private Use Area of ISO/IEC 10646-1:2000 to this standard (ISO/IEC 10646:2003 with Amendment 1) should refer to Standard 2 HKSCS-2004 below.

Standard 2 HKSCS-2004	
Description	The HKSCS-2004 includes 4,941 characters, 123 more characters than the HKSCS-2001. It is technically aligned with the ISO/IEC 10646:2003 with Amendment 1. The HKSCS-2004 specifies the mapping of characters from Private Use Area to the corresponding code points of the ISO/IEC 10646.
Rationale for selection	HKSCS is widely supported by Chinese software in HK.
Maturity	The HKSCS-2004 was released in May 2005 and is available at https://www.ccli.gov.hk/en/archive/terms_hkscs2004.html . Products supporting HKSCS-2004 are available.
Forward outlook	The migration path of IT systems compliant with "ISO/IEC 10646:2003 with Amendment 1 and HKSCS-2004" should be ISO/IEC 10646:2011 or newer versions of the ISO/IEC 10646. Please refer to the Standard 3 ISO/IEC 10646:2011 below for details.
Version and rationale for version	Product support for HKSCS-2004 is already mature.

Standard 2 HKSCS-2004	
Limitations on the use of this standard	The latest version of the HKSCS, namely Hong Kong Supplementary Character Set-2016 (HKSCS-2016), was released in May 2017. Different from previous versions of HKSCS (HKSCS-1999, HKSCS-2001, HKSCS-2004 and HKSCS-2008), HKSCS-2016 includes characters which have already been included in the ISO/IEC 10646 to reflect the actual use of these characters locally. This will not only facilitate the development of vendor support for Chinese characters actually used in HKSAR and the relevant localised technology, but will also reduce the time and cost of development, enabling the IT industry to develop more products suitable for HKSAR. The HKSCS-2016 document is now available at the following web page: https://www.ccli.gov.hk/en/download/terms01.html

Standard 3 ISO/IEC 10646:2011	
Description	ISO/IEC 10646:2011 was published in March 2011. It is a single publication as the result of the merger of the previous releases of ISO/IEC 10646:2003 and its Amendments 1 through 7. ISO/IEC 10646:2011 expands 5 Chinese characters in CJK Unified Ideographs block up to 20,940 characters, contains the same set of Extension A (6,582 characters) and Extension B (42,711 characters) blocks as previous version, and adds Extension C (4,149 characters) and Extension D (222 characters) blocks.
Rationale for selection	ISO/IEC 10646 is ubiquitously supported by numerous IT standards and products, both open source and proprietary. It also gets widespread IT industry support in a wide range of products, which includes operating system, database, office suite, Web browser, software development tool, etc.
Maturity	ISO/IEC 10646:2011 was published in March 2011. It is backward compatible to its previous versions.
Forward outlook	ISO/IEC 10646:2014, ISO/IEC 10646:2017, and ISO/IEC 10646:2020 were released to include CJK Unified Ideographs Extension E (5,762 characters), F (7,473 characters), and G (4,939 characters) blocks respectively in 2014, 2017, and 2020. The latest version of the ISO/IEC 10646 document is freely available at the following website: https://standards.iso.org/ittf/PubliclyAvailableStandards
Version and rationale for version	The selection of the ISO/IEC 10646:2011 provides an appropriate level of flexibility as well as better planning for some IT systems which require these rarely used Chinese characters to be implemented in a standard way, thus achieving the greater interoperability. Although ISO/IEC 10646:2020 is the latest version of the standard, respective font files for supporting this version are not yet available on commonly used IT platforms, including Windows 10 and iOS 14.x.
Limitations on the use of this standard	Comparing with ISO/IEC 10646:2003 with Amendment 1, ISO/IEC 10646:2011 contains ~4,000 (Extension C and D) more ideographic characters, most of them are consolidated from various sources such as Chinese related dictionaries or literatures submitted by regions other than HKSAR. Practically, the default font of operating system may not bundle all the characters included in the ISO/IEC 10646:2011. Project teams need to procure additional fonts for these additional characters on their platforms, while these characters cannot be displayed on other platforms without these additional fonts. Project teams of IT systems which require the interchange of these rarely used characters should take into consideration of the computing environment of the interaction counterparts.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.11 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	ASCII – for encoding content in English	None
ISO/IEC 10646 and HKSCS	ISO/IEC 10646:2003 with Amendment 1 and HKSCS-2004 – for encoding content in English or Chinese (Chinese characters are restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO/IEC 10646 standard and the HKSCS-2004) ISO/IEC 10646:2011 – for encoding content in English or Chinese (Chinese characters are restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO/IEC 10646 standard)	

Remarks:

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).

ISO/IEC 10646 is the standard for the common Chinese language interface. Unicode (ISO/IEC 10646 or UTF-8) shall be adopted for newly developed systems or systems undergoing major revamp with Chinese data content. For details, please refer to "Technical Notes on Website Development and Maintenance", which is available at:

https://www.digitalpolicy.gov.hk/en/our_work/community/web_mobileapp_accessibility/doc/technical_notes.pdf

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

https://www.ccli.gov.hk/en/iso10646/iicore.html.

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/IEC 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 ISO/IEC 10646:2003 with Amendment 1
Please refer to the area "Character sets and encoding for Web content" for details on ISO/IEC 10646:2003 with Amendment 1

Standard 3 HKSCS-2004
Please refer to the area "Character sets and encoding for Web content" for details on HKSCS-2004

Standard 4 ISO/IEC 10646:2011
Please refer to the area "Character sets and encoding for Web content" for details on ISO/IEC 10646:2011

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.12 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	
.gz	.gz v4.3	
.7z	.7z	
.rar	.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	*De facto* 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.
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.

Standard 3 .7z (7-Zip)	
Description	7-Zip is a file archiver with a high compression ratio.
Rationale for selection	It is one of the commonly adopted archive file types.
Maturity	Mature.
Forward outlook	7-Zip will continue to be a commonly utilised file compression format.
Version and rationale for version	Version 9.20 is a stable version since 2010.

Standard 3 .7z (7-Zip)	
Limitations on the use of this standard	None.

Standard 4 .rar	
Description	RAR is a compressed archive file format that supports multipart (multi-volume) archives, several compression/encryption algorithms, and Unicode filenames.
Rationale for selection	It is one of the commonly adopted archive file types.
Maturity	Mature. Developed since 1993.
Forward outlook	Will continue to be a commonly utilised file compression format.
Version and rationale for version	Version 5.0 is the latest stable 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	

3.2.1.13 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
CD-ROM	CD-ROM in ISO 9660:1988 format	None
DVD-ROM	DVD-ROM in ISO/IEC 13346:1995 format	
USB mass storage device	USB mass storage device in FAT format	
Remarks: The FAT format refers to the variants of the file system, namely FAT12, FAT16, FAT32 and exFAT.		

Recommended standards

Standard 1 CD-ROM in ISO 9660:1988 format	
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 organised 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 in ISO/IEC 13346:1995 format	
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

Standard 3 USB mass storage device in FAT format	
Description	A USB mass storage device, which includes but not limited to the USB flash drive and USB hard disk drive, is a data storage device, with an integrated USB interface to become accessible to a host computing device, to enable file transfers between the two. FAT file systems (including FAT12, FAT16, FAT32 and exFAT) are used in the removable media (such as USB flash drives) and supported by various operating platforms.

Standard 3 USB mass storage device in FAT format	
Rationale for selection	Currently, most of the host computing devices, even some mobile devices, support USB mass storage device, where some devices may need to install additional device drivers. Currently, USB mass storage device adopts USB 2.0 or USB 3.0 interface standard to connect to the host computing devices.
Maturity	FAT file system has been a mature standard which was first designed in the late 1970s. The exFAT is the latest file system in the FAT family introduced in 2006 and supported by various operating platforms, such as Microsoft Windows, Linux and Apple Mac OS.
Forward outlook	Will remain popular.
Version and rationale for version	Today, FAT file systems are commonly found on solid-state memory cards, flash memory cards, and on many portable and embedded devices.
Limitations on the use of this standard	The cost and storage capacity of a USB mass storage device is generally higher than that of a floppy diskette, CD-ROM or DVD-ROM. As such, the USB mass storage device may be more appropriate for storing bulky documents and files.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.14 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
HTML5 Apple QuickTime	HTML5 Apple QuickTime (.qt, .mov, .avi)	None

Remarks:
Apple indicated in 2016 that its "QuickTime for Windows" was deprecated and no security updates for the product on Windows platform would be provided. 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 HTML5	
Description	HTML5 is the latest HTML standard. It is bundled with numerous new elements and attributes that enhance semantics, connectivity, performance, device access, 2D and 3D graphics, animation, and styling on the web. With HTML5, animations can now be programmed in the browser. Afterwards, viewers get to enjoy all sorts of animations powered by HTML5, CSS3, and JavaScript. Reference: https://cloudinary.com/blog/creating_html5_animations
Rationale for selection	HTML5 is now widely adopted by majority of websites including those large popular ones (e.g. Google.com, Youtube.com, Yahoo.com and Facebook.com). Reference: https://w3techs.com/technologies/details/ml-html5/all/all
Maturity	HTML 5.2 is a W3C Recommendation by14 December 2017 HTML5 is supported in all modern browsers. In market, there are popular Website Development Tools supporting HTML5 (e.g. Adobe Dreamweaver, Adobe Edge, Microsoft Visio Studio, etc) Reference: https://www.w3.org/TR/html52/ https://www.w3schools.com/html/html5_browsers.asp https://www.adobe.com/devnet/archive/dreamweaver/articles/dw_html5_pt1.html https://www.adobe.com/hk_en/products/edge-animate.html https://visualstudio.microsoft.com/zh-hant/vs/features/web/?rr=https%3A%2F%2Fwww.google.com%2F
Forward outlook	HTML 5.3 is a W3C Working Draft by 18 October 2018 Reference: https://www.w3.org/TR/html53/
Version and rationale for version	HTML 5.2 is the latest version of HTML5.
Limitations on the use of this standard	None

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.
Rationale for selection	Commonly used format for animation on the Web, with freely available players and browser plug-ins.
Maturity	Mature.
Forward outlook	Apple indicated in 2016 that its "QuickTime for Windows" was deprecated and no security updates for the product on Windows platform would be provided. Although Apple has not made official announcement on de-support of QuickTime file format, it is observed that some products in the market started to discontinue the support of QuickTime file format. Content providers shall check the availability of viewer/editor before delivering the content to the receiver.
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	

3.2.1.15 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-4 (ISO 14496) .wav .flac MPEG-2 .mid	MPEG-1 (ISO 11172) – for video and audio .mp3 (ISO 11172) – for audio MPEG-4 (ISO 14496) – for video and audio .wav – for audio .flac – for audio	None
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 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 was approved in 1992.

Standard 2 .mp3	
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).
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	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. 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: • Digital television • Interactive graphics applications (synthetic content) • Interactive multimedia (World Wide Web, distribution of and access to content) Currently, MPEG-4 is divided into 33 parts. The latest part, ISO/IEC 14496-33:2019 – "Information technology - Coding of audio-visual objects - Part 33: Internet video coding" was published in February 2019. 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".
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.

Standard 4 .wav	
Description	Wave format are compatible with most operating systems, it can store high quality sound. Uncompressed wave format is also the standard audio coding for audio CDs.

Standard 4 .wav	
Rationale for selection	Uncompressed wave format can store high quality audio, it is an ideal format for long term archiving and a good choice if future editing is required. Although developed by Microsoft and IBM, its specification is open and there is no licensing associated with it.
Maturity	Initial release of wav format was in 1991. Latest release was in 2007
Forward outlook	None.
Version and rationale for version	Any uncompressed version. Uncompressed wave files are ideal for long term storage and archive.
Limitations on the use of this standard	None.

Standard 5 .flac	
Description	FLAC is a common audio coding format for storing compressed digital audio that is not lossy.
Rationale for selection	FLAC is an open format and is not proprietary. The audio is compressed and the original data can be reconstructed without any data loss.
Maturity	FLAC was originally started in 2000 and later moved to Xiph.org git repository in 2013.
Forward outlook	FLAC is currently being maintained and enhanced.
Version and rationale for version	v1.3.1 , last stable release.
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	MPEG-2 extends the basic MPEG system to provide compression support for TV quality transmission of digital video. 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. In determining the candidate standards it is considered that, in the context of the IF, MPEG-1 and MPEG-4 are sufficient.
.mid	MIDI (Musical Instrument Digital Interface) is a protocol designed for recording and playing back music on digital synthesisers 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. MIDI is not recommended on the basis that sound quality is dependent on the

	capabilities of sound card synthesisers and MPEG-1 and mp3 are the dominant standards for audio on the Internet.

3.2.1.16 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)	None
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 RealAudio/RealVideo (.ra, .ram, .rm, .rmm)	
Description	Proprietary format from Real Networks for receiving streamed content in real time.
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.

Standard 2 Windows Media Formats (.asf, .wma, .wmv)	
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 MPEG-4 (ISO 14496)	
Please refer to the area "Moving image and audio/visual" for details on MPEG-4 (ISO 14496)	

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

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

3.2.1.17 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
JSON	JSON is a lightweight, text-based, language-independent data interchange format. It is based on a subset of the JavaScript programming language standard, ECMA-262 (ISO/IEC 16262) 3rd Edition – December 1999.	
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.

Standard 2 JavaScript Object Notation (JSON)	
Description	JSON is a lightweight, text-based, language-independent data interchange format. It is based on a subset of the JavaScript programming language standard, ECMA-262 (ISO/IEC 16262) 3rd Edition – December 1999.
Rationale for selection	JSON is a lightweight text format that facilitates structured data interchange as an alternative to EXtensible Markup Language (XML). It is supported by NoSQL databases (e.g. CouchDB and MongoDB) and traditional SQL databases (e.g. DB2, MySQL, PostgreSQL, and Oracle). It is language independent and supported by most of the modern programming languages including C, C++, C#, Java, JavaScript, Perl, Python, etc.
Maturity	ECMA-404 "The JSON Data Interchange Format" was published as standard by ECMA in October 2013.
Forward outlook	ECMA will continue to develop ECMA-404 standard.
Version and rationale for version	ECMA-404 is the latest standard published by ECMA for JSON Data Interchange Format.
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	

3.2.1.18 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 1.1 – 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 1.1	
Description	XML Schema defines the structure and content of XML documents. XML Schema 1.1 consists of two parts. (Part 1: Structures and Part 2: Datatypes)
Rationale for selection	XML Schema is a W3C standard. XML Schema is appropriate for data-oriented message exchange and processing.
Maturity	XML Schema 1.1 was approved as a W3C Recommendation on 5 April 2012.
Forward outlook	W3C will continue to develop XML Schema.
Version and rationale for version	Version 1.1 is the 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 (TREX) 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. ISO/IEC 19757-2:2003 was withdrawn and revised by ISO/IEC 19757-2:2008 in December 2008.

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.19 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 Atom	RDF Site Summary (RSS) 1.0 Really Simple Syndication (RSS) 2.0	Atom
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 websites/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.

Standard 1 RSS	
Forward outlook	The number of websites/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.
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.
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	

3.2.1.20 Typography for the Web

Justification for inclusion and usage

The typography for the Web refers to the use, selection and control over the appearances of the fonts on the web pages, aiming at the delivery of a more expressive Web.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Web Open Font Format (WOFF)	Web Open Font Format (WOFF) File Format 1.0 or 2.0	None
Remarks: Proprietary implementation for Web font does not gain wide support from vendors of Web browsers, and hence they are not recommended.		

Recommended standards

Standard 1 Web Open Font Format (WOFF) File Format	
Description	WOFF is a technology for automatically downloading and temporarily installing fonts on demand over the Web, for the display of Web content without requiring the reader to separately download and install fonts to their operating systems.

Standard 1 Web Open Font Format (WOFF) File Format	
Rationale for selection	This standardised technology assists the dissemination of English and Chinese content, particularly rarely used Chinese characters, on the Web through a platform-independent way. In addition, it also enables better typography for the Web and improves the Web accessibility as it can replace those image files that only serve for the purpose of rendering textual content with artistic design.
Maturity	First Public Working Draft (WD) of the WOFF was published by W3C in July 2010. The corresponding Candidate Recommendation (CR) and Proposed Recommendation (PR) were available in August 2011 and October 2012 respectively. The WOFF File Format 1.0 was officially released in December 2012. The WOFF File Format 2.0 was recommended by W3C in March 2018 and its reference implementation can be traced back to 2014.
Forward outlook	More supports from font vendors and Web browsers are perceived.
Version and rationale for version	WOFF File Format 1.0 is a mature version which is supported by major font vendors and Web browsers on desktop and mobile platforms. WOFF File Format 2.0 is the latest recommendation by W3C which provides improved compression of font data and thus lower use of network bandwidth, while still allowing fast decompression even on mobile devices.
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 Calendaring and scheduling information

Justification for inclusion and usage

iCalendar has been a popular format for exchanging calendar information for more than one decade. It is supported by most calendar software including Google Calendar, Hotmail Calendar, Yahoo! Calendar, Microsoft Outlook, Apple iCal, and Lotus Notes. It is a mature standard and has lots of applications support.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
ICS	iCalendar file format (i.e., files with .ics file extension)	None

Remarks:
None.

Recommended standards

Standard 1 iCalendar file format (i.e., files with .ics file extension)	
Description	This document defines the iCalendar data format (i.e., file with .ics file extension) for representing and exchanging calendaring and scheduling information such as events, to-dos, journal entries, and free/busy information, independent of any particular calendar service or protocol.
Rationale for selection	iCalendar is supported by a large number of products, including Google Calendar, Apple Calendar, IBM Lotus Notes, Microsoft Outlook, and is commonly used for scheduling event within Government as well as between Government and external parties.
Maturity	The first version of iCalendar specification (RFC 2445) was published by the IETF in November 1998 to specify an Internet standards track protocol for the Internet community. In September 2009, RFC 5545 was published by the IETF, making RFC 2445 obsolete.
Forward outlook	The specification is subject to further developments. For example, new standard were proposed in 2009 and 2013 by RFC5546 and RFC6868, respectively.
Version and rationale for version	RFC 5545 is the current version of iCalendar specification.
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	

3.2.1.22 Physical or Digital object event creation and sharing

Justification for inclusion and usage

The goal of Electronic Product Code Information Services (EPCIS) is to enable disparate applications to create and share visibility event data, both within and across enterprises. Ultimately, this sharing is aimed at enabling users to gain a shared view of physical or digital objects within a relevant business context.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
ISO/IEC 19987:2017	ISO/IEC 19987:2017 EPC Information Services (EPCIS) Standard	None
Remarks: None		

Recommended standards

Standard 1 ISO/IEC 19987:2017 EPC Information Services (EPCIS) Standard	
Description	The goal of EPCIS is to enable disparate applications to create and share visibility event data, both within and across enterprises. Ultimately, this sharing is aimed at enabling users to gain a shared view of physical or digital objects within a relevant business context. EPCIS provides open, standardised interfaces that allow for seamless integration of well-defined services in inter-company environments as well as within companies. Standard interfaces are defined in the EPCIS standard to enable visibility event data to be captured and queried using a defined set of service operations and associated data standards, all combined with appropriate security mechanisms that satisfy the needs of user companies. In many or most cases, this will involve the use of one or more persistent databases of visibility event data, though elements of the Services approach could be used for direct application-to-application sharing without persistent databases. With or without persistent databases, the EPCIS specification specifies only a standard data sharing interface between applications that capture visibility event data and those that need access to it. It does not specify how the service operations or databases themselves should be implemented. This includes not defining how the EPCIS services should acquire and/or compute the data they need, except to the extent the data is captured using the standard EPCIS capture operations. The interfaces are needed for interoperability, while the implementations allow for competition among those providing the technology and implementing the standard.
Rationale for selection	EPCIS is backed by cross countries, and cross industries. • EPCIS is the only global interoperability standard defined for event sharing across companies as well as industries. • EPCIS is being widely adopted by various industries and operations including but not limited to trading, logistics, food, medical, government. • Innovation and Technology Commission of HKSAR Government sponsored world first EPCIS infrastructure development in 2005. • EPCIS is implementation independent, and it only defines the interoperability message between systems. • EPCIS conforms to HKSARG IF using SOAP.
Maturity	EPCIS v1.0 was ratified in 2007. EPCIS v1.1 was ratified in 2014. EPCIS v1.1 was published as ISO/IEC19987:2015. EPCIS v1.2 was published as ISO/IEC 19987:2017 in October 2017.
Forward outlook	EPCIS standards development will continue to be led by GS1, with the participation from experts in cross industry globally.
Version and rationale for version	ISO/IEC 19987:2017 is a mature version which is completely identical to EPCIS 1.2 ratified in 2017.
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 Digital Geographic Data, Metadata and Geospatial Web Services

Justification for inclusion and usage

Geographic Data is data with implicit and/or explicit reference to a location on Earth. These data have been commonly created, stored, processed and exchanged in digital format. They have been used in a wide range of applications, such as topographic mapping, cadastral survey, town planning, housing development, civil engineering works, census, election, public health, transportation and tourism.

Metadata provides information about data like identification, spatial extents, use constraints and distribution methods. It facilitates the discovery, access, retreival and use of Geographic Data.

Geospatial Web Services provide a way for users to access and exchange Geographic Data, map images and Metadata over the web.

As announced in the 2017 Policy Address, the Government acknowledged its commitment in striving to promote the establishment of Common Spatial Data Infrastructure (CSDI). The core concept of CSDI is to make Geographic Data, Metadata and Geospatial Web Services interoperable and as such standardisation is necessary.

Additionally, different themes or sources of Geographic Data with Common Reference System (CRS) can be overlaid for composite maps, spatial analysis or other geospatial applications. CRS defined in ISO 19111:2019 specifies the required data elements, relationships and associated metadata for spatial referencing. It also enables the implementation of coordinate conversion or coordinate transformation to bring Geographic Data in different coordinate reference systems into a unified one. The Survey and Mapping Office, Lands Department is responsible to define the local Coordinate Reference Systems, and to publish and maintain the relevant official parameters describing the local CRS for government and public users from time to time.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
GML GeoJSON GeoTIFF ISO 19115 ISO/TS 19139 OGC Web Services Standards ISO 19111:2019 OGC APIs	GML 3.1.1 (no ISO standard) and 3.2.1 (equivalent to ISO 19136:2007) Geography JavaScript Object Notation (GeoJSON - RFC 7946) GeoTIFF 1.1 Specification ISO 19115:2003 (Geographic information — Metadata) ISO/TS 19139:2007 (Geographic information — Metadata — XML schema implementation) OGC Web Services Standards: - OGC Web Map Service (WMS) 1.1.1 and 1.3.0 - OGC Web Map Tile Service (WMTS) 1.0.0 - OGC Web Feature Service (WFS) 1.0.0, 1.1.0 and 2.0.0 - OGC Web Coverage Service (WCS) 1.0.0, 1.1.0, 1.1.1, 1.1.2 and 2.0.1 - OGC Web Processing Service (WPS) 1.0.0 - OGC Catalogue Service for the Web (CSW) 2.0.2 ISO 19111:2019 (Geographic information -- Spatial referencing by coordinates)	GML 3.3 (equivalent to ISO 19136-2:2015) ISO 19115-1:2014 (Geographic information — Metadata — Part 1: Fundamentals) ISO 19115-2:2019 (Geographic information — Metadata — Part 2: Extensions for acquisition and processing) ISO/TS 19115-3:2016 (Geographic information — Metadata — Part 3: XML schema implementation for fundamental concepts) OGC APIs

Remarks:

The above open Geographic Data formats, Metadata and Geospatial Web Services standards are recongised by the International Organization for Standardization (ISO) and/or the Open Geospatial Consortium (OGC).

In the long term, under the CSDI strategic framework, B/Ds are required to progressively release spatial data in compliance with the CSDI standards to the public through the CSDI Portal. For detail, B/Ds should refer to Development Bureau General Circular No. 1/2021 and CSDI Resources Centre at https://geoportal.landsd.ccgo.hksarg/csdi/main/ (Intranet).

Recommended standards

Standard 1 Geographic Markup Language (GML) (no ISO standard) 3.1.1 and 3.2.1 (equivalent to ISO 19136:2007)	
Description	The GML is an Extensible Markup Language (XML) grammar for expressing geographical features. It is defined by the Open Geospatial Consortium (OGC), which aims to advance the development and use of international standards and supporting services that promote geospatial interoperability (http://www.opengeospatial.org/standards/gml). GML serves as a modelling language for geographic systems, as well as an open interchange format, for geographic transactions on the Internet.

Standard 1 Geographic Markup Language (GML) (no ISO standard) 3.1.1 and 3.2.1 (equivalent to ISO 19136:2007)	
Rationale for selection	As GML is built on a widely adopted public standard, namely XML, data encoded by GML can be viewed, edited and transformed by a wide variety of commercial and free software tools, such as ArcGIS, GeoServer, OpenLayers, Quantum GIS, andGRASS GIS, etc. The use of GML can facilitate the development of open sharing and interchange of geographic information. Another example is that the Survey and Mapping Office (SMO) of the Lands Department of the Government of the Hong Kong Special Administrative Region has adopted the use of GML version 3.1.1 for their digital maps.
Maturity	GML 3.1.1 and 3.2.1 were approved in 2004 and 2007 respectively.
Forward outlook	GML 3.3 was released to provide additional schema components based on GML 3.2. The need for this version will be considered in the future. The OGC and the OGC GML Working Group (WG) are collecting the views from the user communities, OSGeo, developers and ISO/TC211 members on the development of GML 4.0 on top of adopted GML 3.2/3.3.
Version and rationale for version	GML 3.1.1 and 3.2.1 are recommended as they are still the versions with wide industry adoption.
Limitations on the use of this standard	None

Standard 2 Geography JavaScript Object Notation (GeoJSON - RFC 7946)	
Description	GeoJSON is a geo-spatial data interchange format based on JSON and is supported by some commonly used Geographic Information System (GIS)/map servers.
Rationale for selection	GeoJSON – RFC7946 was recommended in the Final Report of consultancy study called "*Establishment of Data Standards for Framework Spatial Data and Design of Process, Mechanism and Architecture of a Common Spatial Data Infrastructure (CSDI) Platform*" commissioned by Lands Department of the Government of the Hong Kong Special Administrative Region. This is one of the open geo-spatial data formats for data exchange and sharing through the web.
Maturity	RFC 7946 was proposed in August 2016.
Forward outlook	The newer standard specification (RFC 7946) has been further revised since 2016. For details please refer to https://geojson.org/
Version and rationale for version	RFC 7946
Limitations on the use of this standard	None
Standard 3 Geo-referenced Tagged Image File Format (GeoTIFF) 1.1 Specification	
Description	GeoTIFF is a public domain metadata standard which allows georeferencing information to be embedded within a TIFF (Tagged-Image File Format) file. The latest official release version is GeoTIFF v1.1 Specification which was released in September 2019 (https://www.ogc.org/standards/geotiff). GeoTIFF defines a set of TIFF tags that describe cartographic information associated with TIFF imagery from satellite imaging systems, scanned aerial photography, scanned maps, digital elevation models, or geographic analyses. It allows means for tying a raster image to a known model space or map projection, and for describing those projections.

Standard 2 Geography JavaScript Object Notation (GeoJSON - RFC 7946)	
Rationale for selection	GeoTIFF is a joint development effort involved over 160 remote sensing, GIS, cartographic, and surveying related companies and organisations. It is supported by several GIS software such as Python Imaging Library (PIL), ArcInfo, ERDAS IMAGINE, PCI EASI/PACE, etc. Another example is that the Survey and Mapping Office (SMO) of the Lands Department of the Government of the Hong Kong Special Administrative Region has adopted the use of GeoTIFF for their digital maps and digital orthophotos..
Maturity	GeoTIFF 1.1 Specification was released in September 2019.
Forward outlook	OGC will continue to develop GeoTIFF 1.1.
Version and rationale for version	GeoTIFF 1.1 Specification is the latest official release version.
Limitations on the use of this standard	None

Standard 4 ISO 19115:2003 (Geographic information — Metadata)	
Description	ISO 19115:2003 defines the schema required for describing geographic information by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal schema, spatial reference, and distribution of digital geographic data.
Rationale for selection	Given the wide recognition and adoption of this international metadata standard in the market of the geospatial industry today, this standard was recommended in the Final Report of consultancy study called "*Establishment of Data Standards for Framework Spatial Data and Design of Process, Mechanism and Architecture of a Common Spatial Data Infrastructure (CSDI) Platform*" commissioned by Lands Department of the Government of the Hong Kong Special Administrative Region, and decided to be adopted to ensure the interoperability among IT/GIS and catalogue systems.
Maturity	ISO 19115-1:2003 is widely adopted by many overseas IT/GIS and catalogue systems of spatial data infrastructure (SDI) portals.
Forward outlook	The adopted standards shall be reviewed in the future to determine the necessity of applying the newer standards, such as ISO 19115-1:2014.
Version and rationale for version	ISO 19115:2003 is recommended as this is widely adopted in different IT/GIS and catalogue systems of SDI portals.
Limitations on the use of this standard	None

Standard 5 ISO/TS 19139:2007 (Geographic information — Metadata — XML schema implementation)	
Description	ISO/TS 19139:2007 defines the encoding rules for implementing the conceptual model of ISO 19115:2003 in XML format.
Rationale for selection	The metadata based on the conceptual model of ISO 19115:2003 shall be encoded in XML format so as to be machine-readable.
Maturity	ISO 19139:2007 is widely adopted by many overseas IT/GIS and catalogue systems of spatial data infrastructure (SDI) portals.
Forward outlook	The adopted standards shall be reviewed in the future to determine the necessity of applying the newer standards, such as ISO 19115-3:2016.

Standard 5 ISO/TS 19139:2007 (Geographic information — Metadata — XML schema implementation)	
Version and rationale for version	ISO 19139:2007 is recommended as this is widely adopted in different IT/GIS and catalogue systems of SDI portals.
Limitations on the use of this standard	None

Standard 6a OGC Web Map Service (WMS) 1.1.1 and 1.3.0	
Description	OGC WMS is an open standard which defines the standard HTTP interface for requesting geo-referenced map images from a GIS server.
Rationale for selection	This standard interface can greatly improve the interoperability of the provision of map visualisation service. Customisation of the map style is also supported by this service.
Maturity	OGC WMS 1.1.1 and 1.3.0 were published in 2002 and 2004 respectively.
Forward outlook	To further improve the interoperability and usability of geospatial data on the web, OGC is currently developing an OGC API family of standards which are built upon the existing OGC Web Service standards (WMS, WFS, WCS, WPS, etc.).
Version and rationale for version	OGC WMS 1.1.1 and 1.3.0 are widely adopted and supported.
Limitations on the use of this standard	None

Standard 6b OGC Web Map Tile Service (WMTS) 1.0.0	
Description	OGC WMTS is an open standard which defines the standard HTTP interface for requesting static geo-referenced map image tiles from a GIS server.
Rationale for selection	OGC WMTS also serve the purpose of improving the interoperability of map visualisation service. Comparing with OGC WMS, the static map image tiles served by WMTS can be pre-rendered and pre-cache on the server-side, and thus this improves the service performance and is suitable for serving numerous users.
Maturity	OGC WMTS 1.0.0 was released in 2010
Forward outlook	To further improve the interoperability and usability of geospatial data on the web, OGC is currently developing an OGC API family of standards which are built upon the existing OGC Web Service standards (WMS, WFS, WCS, WPS, etc.).
Version and rationale for version	OGC WMTS 1.0.0 is the only version currently available.
Limitations on the use of this standard	None

Standard 6c OGC Web Feature Service (WFS) 1.0.0, 1.1.0 and 2.0.0	
Description	OGC WFS is an open standard which defines the standard HTTP interface for questing vector geographic features (point, line and polygon).
Rationale for selection	This standard interface can improve the exchange and interoperability of vector geographic data.
Maturity	OGC WFS 1.0.0, 1.1.0 and 2.0.0 were published in 2002, 2005 and 2010 respectively.

Standard 6c OGC Web Feature Service (WFS) 1.0.0, 1.1.0 and 2.0.0	
Forward outlook	To further improve the interoperability and usability of geospatial data on the web, OGC is currently developing an OGC API family of standards which are built upon the existing OGC Web Service standards (WMS, WFS, WCS, WPS, etc.). Of these, OGC API - Features - Part 1: Core, which was formerly known as WFS 3.0, was approved and published in 2019.
Version and rationale for version	OGC WFS 1.0.0, 1.1.0 and 2.0.0 are widely adopted and supported.
Limitations on the use of this standard	None

Standard 6d OGC Web Coverage Service (WCS) 1.0.0, 1.1.0, 1.1.1, 1.1.2, and 2.0.1	
Description	OGC WCS is an open standard which defines the standard HTTP interface for requesting raster geographic coverage data, such as digital elevation data, satellite images and other raster data containing values at each pixel.
Rationale for selection	This standard interface can improve the exchange and interoperability of raster geographic coverage data.
Maturity	OGC WCS 1.0.0, 1.1.0, 1.1.1, 1.1.2, and 2.0.1 were approved and published by OGC.
Forward outlook	To further improve the interoperability and usability of geospatial data on the web, OGC is currently developing an OGC API family of standards which are built upon the existing OGC Web Service standards (WMS, WFS, WCS, WPS, etc.).
Version and rationale for version	OGC WCS 1.0.0, 1.1.0, 1.1.1, 1.1.2, and 2.0.1 are widely adopted and supported
Limitations on the use of this standard	None

Standard 6e OGC Web Processing Service (WPS) 1.0.0	
Description	OGC WCS is an open standard which defines the standard HTTP interface for standardising inputs and outputs (or known as requests and responses) of geospatial processing services. The processes can include any algorithm, calculation or model that operates on geo-referenced vector or raster data.
Rationale for selection	It provides easy and interoperable access to various geospatial vector and raster processes.
Maturity	OGC WPS 1.0.0 was published in 2007.
Forward outlook	To further improve the interoperability and usability of geospatial data on the web, OGC is currently developing an OGC API family of standards which are built upon the existing OGC Web Service standards (WMS, WFS, WCS, WPS, etc.).
Version and rationale for version	OGC WPS 1.0.0 is widely adopted and supported.
Limitations on the use of this standard	None

Standard 6f OGC Catalogue Service for the Web (CSW) 2.0.2	
Description	OGC CSW defines the standard HTTP interface for publishing and searching collections of Metadata about geospatial data and services and related resource information. Resource provider can use catalogues to register metadata that conform to the information model that CSW supports. The metadata shall conform to ISO 19115 and ISO 19139 standards.
Rationale for selection	Metadata registered in the catalogue can be queried and returned through the CSW for resource evaluation. This enables the discovery of Geographic Data and Geospatial Web Services.
Maturity	OGC CSW 2.0.2 was published in 2007.
Forward outlook	To further improve the interoperability and usability of geospatial data on the web, OGC is currently developing an OGC API family of standards which are built upon the existing OGC Web Service standards (WMS, WFS, WCS, WPS, etc.).
Version and rationale for version	OGC CSW 2.0.2 is widely adopted and supported.
Limitations on the use of this standard	None.

Standard 7 ISO 19111:2019 (Geographic information -- Spatial referencing by coordinates)	
Description	ISO 19111:2019 defines the conceptual schema for the description of spatial referencing by coordinates, optionally extended to spatio-temporal referencing. It describes the minimum data required to define one-, two- and three-dimensional spatial coordinate reference systems with an extension to merged spatial-temporal reference systems. It allows additional descriptive information to be provided. It also describes the information required to change coordinates from one coordinate reference system to another.

Standard 7 ISO 19111:2019 (Geographic information -- Spatial referencing by coordinates)	
Rationale for selection	ISO 19111:2019 is applicable to producers and users of geographic information. Although it is applicable to digital geographic data, its principles can be extended to many other forms of geographic data such as maps, charts and text documents. The Survey and Mapping Office (SMO), Lands Department is responsible to define the local Coordinate Reference Systems (CRS), and to publish and maintain the relevant official parameters describing the local CRS for government and general public users from time to time. The suggested ISO19111:2019 (Geographic information – Referencing by Coordinates) includes the up-to-date and required parameters to enhance the description of the geo-spatial features on the Earth, including: • inclusion of applicable modern geodetic terminology; • extension to describe dynamic geodetic reference frames; • extension to describe geoid-based vertical coordinate reference systems; • extension to allow triaxial ellipsoid for planetary applications; • extension to describe three-dimensional projected coordinate reference systems; • addition of 'datum ensembles' to allow grouping of related realisations of a reference frame where for lower accuracy applications the differences are insignificant; • clarification in the modelling of derived coordinate reference systems; • remodelling of the metadata elements scope and extent; • addition of requirements to describe coordinate metadata and the relationship between spatial coordinates; • additional modelling of temporal coordinate reference system components sufficient for spatio-temporal coordinate referencing; • consolidation of the provisions of ISO 19111-2:2009 (Spatial referencing by coordinates — Extension for parametric values) into this document; • change in name from 'Spatial referencing by coordinates' to 'Referencing by coordinates', due to the inclusion of the non-spatial coordinate reference system subtypes of parametric (from ISO 19111-2) and temporal; • the correction of minor errors.
Maturity	ISO 19111:2019 was last reviewed and confirmed in 2019.
Forward outlook	ISO will continue to develop ISO 19111:2019.
Version and rationale for version	ISO 19111:2019 was the latest version published by ISO.
Limitations on the use of this standard	None

Emerging standards for future consideration

Emerging Standard(s)	Description
GML 3.3 (equivalent to ISO 19136-2:2015)	GML 3.3 is an extension to GML 3.2 which provides additional schema components. For example, a new encoding of Triangulated Irregular Networks (TINs) is formulated in version 3.3. Note: GML 3.3 is backwards compatible with GML 3.2.
ISO 19115-1:2014 (Geographic information — Metadata — Part 1: Fundamentals)	ISO 19115-1:2014 defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services. Note: ISO 19115-1:2014 is backwards compatible with ISO 19115:2003
ISO 19115-2:2019 (Geographic information — Metadata — Part 2: Extensions for acquisition and processing)	ISO 19115-2:2019 is an extension of ISO 19115-1 to describe the acquisition and processing of geographic information from all sources, including but not limited to imagery and gridded data.
ISO/TS 19115-3:2016 (Geographic information — Metadata — Part 3: XML schema implementation for fundamental concepts)	ISO/TS 19115-3:2016 defines an integrated XML implementation for ISO 19115-1:2014 and ISO 19115-2:2019.
OGC APIs	OGC API family of standards are built upon the existing OGC Web Service standards (WMS, WFS, WCS, WPS, etc.). It makes use of the OpenAPI Specification and defines a language-agnostic interface for Geospatial Web Service that allows humans and computers to easily discover and understand the capabilities of the services, and could therefore improve the accessibility of the Geospatial Web Service. OGC API - Features - Part 1: Core and Part 2: Coordinate Reference Systems by Reference were approved in 2019 and 2020 respectively. The remaining OGC APIs are still being developed.

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.24 Quick Response (QR) Code

Justification for inclusion and usage

Since the invention of QR code in 1994 with the aim of tracking vehicles during manufacturing process, it has expanded beyond the initial industrial tracking purpose progressively. Nowadays, it is used by the general public to display text, add vCard contact, open web page, make on-line payment, join social network, obtain promotion offer, etc.

The use of QR code is becoming more popular in recent years because of the higher usage rate of camera-embedded mobile devices, together with the wide availability of mobile apps that equipped with QR code scanning capability.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
ISO/IEC 18004:2015	ISO/IEC 18004:2015	None
Remarks: None.		

Recommended standards

Standard 1 ISO/IEC 18004:2015	
Description	ISO/IEC 18004:2015 standard defines the requirements for the symbology known as QR Code. It specifies the QR Code symbology characteristics, data character encoding methods, symbol formats, dimensional characteristics, error correction rules, reference decoding algorithm, production quality requirements, and user-selectable application parameters (http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62021)
Rationale for selection	QR codes provide the features of high capacity encoding of data, small printout size, readable from any direction in 360 degree, and dirt and damage resistant.
Maturity	ISO/IEC 18004:2015 standard was published on 16 February 2015.
Forward outlook	ISO/IEC will continue to develop ISO/IEC 18004:2015 standard.
Version and rationale for version	ISO/IEC 18004:2015 standard is the latest version published by ISO/IEC.
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	

3.2.1.25 Sensor Information Exchange

Justification for inclusion and usage

The Sensor Information Exchange interoperability area helps to define the data interchange format required for communicating and exchanging information between different sensors across diverse and heterogeneous networks. Such formats can help to assist that sensor data can be better understood by machines, and processed automatically in complex workflows, and easily shared between applications such as Internet of Things (IoT).

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Sensor Web Enablement (SWE) Common Data Model Encoding	Sensor Web Enablement (SWE) Common Data Model Encoding v2.0	
Remarks: None.		

Recommended standards

Standard 1 Sensor Web Enablement (SWE) Common Data Model Encoding v2.0	
Description	It defines low-level sensor related datasets descriptions to fully describe sensor data stream, namely, representation, nature, structure and encoding in a self-describing and semantically enabled way. It defines normative Unified Modelling Language (UML) models with which derived encoding models should be compliant, and also a normative XML grammar and a set of patterns for the implementation of such models.
Rationale for selection	The standard is mature and commonly adopted by the industry (e.g. deployments under the U.S. Integrated Ocean Observing System and open source community OpenSensorHub) Reference: https://ioos.github.io/sos-guidelines/sos-wsdd-1-0.html https://asprspotomac.org/2015geotech/presentations/GeoTech2015-Botts.pdf
Maturity	SWE Common Data Model Encoding v2.0 was approved in 2011.
Forward outlook	SWE Common Data Model Encoding version 2.0 was published in 2011, and hence it is mature enough to be included under the Information Access and Interchange domain.
Version and rationale for version	None
Limitations on the use of this standard	None

Emerging standards for future consideration

Emerging Standard(s)	Description

Other candidate standards

Other Standard(s)	Description
None	

3.2.1.26 Media delivery interface for the Web

Justification for inclusion and usage

An Application Programming Interface (API) that allows playback of protected content in Web browsers.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Encrypted Media Extensions	Encrypted Media Extensions (EME)	None
Remarks: None.		

Recommended standards

Standard 1 Encrypted Media Extensions (EME)	
Description	The HTML Media Extensions Working Group published Encrypted Media Extensions (EME) as a W3C Recommendation which extends the 'HTMLMediaElement' element of the HTML specification. EME is an Application Programming Interface (API) that allows playback of protected content in Web browsers. W3C's Media Source Extensions (MSE) provides the API for streaming video while EME provides the API for handling encrypted content. The combination of MSE and EME is the most common practice to deliver commercial quality video over the Web.
Rationale for selection	EME offers a better user experience, bringing greater interoperability, privacy, security and accessibility to viewing encrypted video on the Web. The EME specification has been developed with a focus on the security and privacy of the user. Compared to previous methods of viewing encrypted video on the Web, EME has the benefit that all interactions happen within the browser. EME moves the responsibility for interaction with encrypted video from plugins to the browser, which acts as a true user agent.
Maturity	EME standard was published by W3C on 18 September 2017, which has been implemented in major Web browsers.
Forward outlook	More supports from Web browsers are perceived and W3C will continue to develop EME standard.
Version and rationale for version	The EME standard published on 18 September 2017 is the latest version recommended by W3C.

Standard 1 Encrypted Media Extensions (EME)	
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	

3.2.1.27 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.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Scalable Vector Graphics	Scalable Vector Graphics v1.0 or v1.1	None
Remarks: None.		

Recommended standards

Standard 1 Scalable Vector Graphics v1.0 or v1.1	
Description	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. 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. SVG is also suitable for display on mobile devices (using SVG Mobile Profiles).
Rationale for selection	SVG is wildly adopted in many large popular websites (e.g. Google.com, Youtube.com, Yahoo.com and Twitter.com) and commonly used in the industry. Reference: https://w3techs.com/technologies/details/im-svg/all/all
Maturity	Scalable Vector Graphics (SVG) 1.1 (Second Edition) was published on 16 August 2011. All major modern web browsers—including Mozilla Firefox,, Google Chrome, Opera, Safari, and Microsoft Edge—have SVG rendering support. Moreover, various applications in market are now supporting SVG, like Adobe Illustrator, CorelDraw, Inkscape, etc. Reference: https://www.w3.org/TR/SVG11/ http://svgtutorial.com/svg-browser-support/ https://www.adobe.com/search.html#q=svg&sort=relevancy&start=1 https://learn.corel.com/?s=svg https://inkscape.org/search/?q=svg
Forward outlook	The W3C is working on development of SVG v2 which was as a W3C Candidate Recommendation on 4 October 2018. SVG v2 will add new ease-of-use features to SVG. Reference: https://svgwg.org/svg2-draft/single-page.html
Version and rationale for version	SVG v1.0 was approved as a W3C Recommendation in September 2001 and SVG v1.1 (Second Edition) was approved as a W3C Recommendation in August 2011.
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	

3.2.2 Interoperability areas for future consideration – no apparent need yet

3.2.2.1 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	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. 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. 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. 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. The RDF suite of specifications consists of a number of components:

Standard(s)	Description
	• 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 • rdf:PlainLiteral: A Datatype for RDF Plain Literals (Second Edition) In addition, the SPARQL is the standard which specifies the languages and protocols to query and manipulate RDF graph content on the Web or in an RDF store. It was released as a W3C Recommendation, as SPARQL 1.0, in January of 2008. The current version, SPARQL 1.1, became a W3C Recommendation in March 2013. The SPARQL 1.1 standard comprises the following specifications: • SPARQL 1.1 Query Language • SPARQL 1.1 Query Results JSON Format and SPARQL 1.1 Query Results CSV and TSV Formats • SPARQL 1.1 Federated Query • SPARQL 1.1 Entailment Regimes • SPARQL 1.1 Update Language • SPARQL 1.1 Protocol for RDF • SPARQL 1.1 Service Description • SPARQL 1.1 Graph Store HTTP Protocol • SPARQL 1.1 Test Cases

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

EPCglobal Standard(s)	Description
The suite of RFID related specifications from EPCglobal *(see the specific standards listed below in this table)*	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. The Electronic Product Code (EPC) is a unique number that identifies a specific item in the supply chain. EPC is promoted by EPCglobal. 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. The International Standards Organisation (ISO) has approved the EPC Gen2 Class 1 UHF standard to its 18000-6C standard in July 2006. ISO is working on standards for tracking goods in supply chain using high-frequency tags (ISO 18000-3) and ultra-high frequency tags (ISO 18000-6). In some cases, the implementation of RFID solutions with the full suite of specifications may not be necessary. At present, the suite comprises the following specifications :
EPC Tag Data Specification	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.EPC Tag Data Specification Version 1.13 was released by EPCglobal on November 2019. The EPC Tag Data Specification version 1.13 applies to RFID tags conforming to EPC Gen2 Class 1 UHF standard at 860 MHz-960MHz. It encompasses the specific encoding schemes including a General Identifier (GID), a serialised version of the Global Trade Item Number (GTIN), GTIN + Batch/Lot (LGTIN), the Serial Shipping Container Code (SSCC), the Global Location Number (GLN), the Global Returnable Asset Identifier (GRAI), the Global Individual Asset Identifier (GIAI), the Global Service Relation Number - Recipient (GSRN), Global Service Relation Number – Provider (GSRNP),Component / Part Identifier (CPI), Serialized Global Coupon Number (SGCN), Individual Trade Item Piece (ITIP), the Global Document Type Identifier (GDTI), the Aerospace and Defense Identifier (ADI) and the US Department of Defense Identifier (DOD). Apart from the above encoding schemes, it also defined the following schemes to support product identification: the Global Identification Number for Consignment (GINC), the Global Shipment Identification Number (GSIN), the Unit Pack Identifier (UPUI), the Global Location Number of Party (PGLN), the BIC Container Code (BIC), and the IMO Vessel Number (IMOVN).

EPCglobal Standard(s)	Description
Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz	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. The former OFTA approved a dual-band frequency (865-868MHz and 920-925MHz) for UHF RFID application in HK. The version 2.0.0 features a number of backwards-compatible, optional features including: • Untraceable function to hide portions of data, restrict access privileges and reduce a tag's read range. • Support for cryptographic authentication of tags and readers to verify identity and provenance, as well as reduce the risk of counterfeiting and unauthorised access. • Enhanced User Memory for "Alteration EAS" and supplementary encodings (such as maintenance logging) during a product's life cycle. "Non-removable" flag for embedded tagging of electronics and sewn-in tagging of apparel, to indicate that a tag cannot easily be removed without compromising the tagged product's intended functionality.
Reader Protocol Standard	This specification defines the communication messaging and protocol between tag readers and EPC compliant software applications.
Application Level Event (ALE) Specification	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.
Object Naming Service (ONS) Specification	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 websites 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	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).

ISO Standard(s)	Description
ISO 18000 series of standards (Radio frequency identification for item management)	The ISO 18000 is a series of standards that define the air interface for the different RFID frequencies in use around the globe. It was approved by ISO from 2009 to 2014 covering different air interfaces for globally accepted frequencies, including low frequency, high frequency and ultrahigh frequency as indicated below. • ISO/IEC 18000-2:2009 : Air interface communications below 135 kHz (https://www.iso.org/standard/46146.html) • ISO/IEC 18000-3:2010 : Air interface communications at 13.56 MHz (https://www.iso.org/standard/53424.html) • ISO/IEC 18000-4:2015 : Air interface communications at 2.45 GHz (https://www.iso.org/standard/62539.html) • ISO/IEC 18000-6:2013 : Air interface communications at 860 MHz to 930 MHz (https://www.iso.org/standard/59644.html) • ISO/IEC 18000-7:2014 : Air interface communications at 433.92 MHz (https://www.iso.org/standard/57336.html)

3.2.3.2 Efficient XML Interchange (EXI)

Justification for inclusion and usage

Efficient XML Interchange (EXI) is a binary XML format for exchange of data on a computer network. It was developed by the W3C's Efficient Extensible Interchange Working Group and is one of the most prominent binary XML efforts to encode XML documents in a binary data format, rather than plain text. Using EXI format reduces the verbosity of XML documents as well as the cost of parsing. Improvements in the performance of writing (generating) content depends on the speed of the medium being written to, the methods and quality of actual implementations.

Remarks:

EXI provides a very compact representation for the Extensible Markup Language (XML) information, and hence is able to optimise performance and the utilisation of computational resources.

For example, in the scenario of Internet of Things (IoT), in which Extensible Messaging and Presence Protocol (XMPP) is often used as a communication protocol, EXI binding can be applied to XMPP for those small devices in resource constrained networks. This can result in a compression of data being transmitted, and therefore enable sensors with limited memory to communicate efficiently.

Standards for future consideration

Standard(s)	Description
EXI	EXI format v1.0 was approved by W3C in 2014. It is still subject to development by W3C in recent years. In the field of IoT, EXI simultaneously improves performance and significantly reduces bandwidth requirements without compromising efficient use of other resources such as battery life, code size, processing power, and memory.

3.2.3.3 Media Application Format

Justification for inclusion and usage

A multimedia format optimised for streaming delivery and decoding on end user devices in adaptive multimedia presentations.

Remarks:

None.

Standards for future consideration

Standard(s)	Description
ISO/IEC 23000-19	The full name for this standard is ISO/IEC 23000-19 (Information technology -- Multimedia application format (MPEG-A) - Part 19: Common Multimedia Application Format (CMAF) for segmented media). CMAF combines and constrains several MPEG specifications to define a multimedia format that is optimised for delivery of a single adaptive multimedia presentation to a variety of devices, using a variety of adaptive streaming, broadcast, download, and storage methods. CMAF provides a common media specification that application specifications, such as MPEG Dynamic Adaptive Streaming over HTTP (DASH), can reference and a common media format that allows a single encoded multimedia presentation to be used by many applications. The committee draft of the CMAF specification was released by the Motion Picture Experts Group (MPEG) in June 2016. ISO/IEC 23000-19:2018, which specifies the CMAF multimedia format, was published in January 2018. ISO/IEC 23000-19:2018 was withdrawn and revised by ISO/IEC 23000-19:2020 in March 2020.

3.3 SECURITY DOMAIN

3.3.1 Interoperability areas for immediate consideration

3.3.1.1 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 1.1 or WS-Security 1.1.1	None
Remarks: Project teams should closely monitor the development of the OASIS Web Services Security Maintenance (WSS-M) TC and follow its recommendations when it is ratified.		

Recommended standards

Standard 1 WS-Security 1.1 or WS-Security 1.1.1	
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. WS-Security 1.1 was approved as an OASIS standard in February 2006. It includes the following new features: • Encrypted SOAP Header • Token Reference to Encrypted Key • Signature Confirmation • Password-based Key Derivation • Thumbprint References Web Services Security 1.1.1 was approved as an OASIS standard in June 2012. The WS-Security 1.1.1 specification set integrated specific error corrections and editorial changes to the preceding 1.1 specifications. It does not add any new features beyond those of the base specifications version 1.1.
Rationale for selection	WS-Security v1.1 and v1.1.1 are OASIS standards, and are industry-wide recognised XML-based standards for securing Web Services message exchanges. WS-Security 1.1.1 and 1.1 are backward compatible with 1.0.
Maturity	Web Services Security (WS-Security) version 1.1 has become an OASIS standard in November 2006. It is supported by major platform development providers such as Oracle, IBM and Microsoft. It is also supported in security products such as Verisign's Trust Gateway and WebSphere Application Server.
Forward outlook	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. 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.
Version and rationale for version	WS-Security is a mature standard.
Limitations on the use of this standard	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. The progress of the OASIS Web Services Security Maintenance (WSS-M) TC (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss-m) which focuses on ongoing maintenance on WS-Security 1.1 and token profiles should be closely monitored.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.3.1.2 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 CMS (RFC 5652)	PKCS #7 v1.5 (RFC 2315) S/MIME v3 or v4 PDF v1.5, 1.6, 1.7 (ISO 32000-1) or 2.0 (ISO 32000-2:2020)	CMS (RFC 5652)
Remarks: For electronic submissions via e-mail pursuant to the ETO, members of the public should use only those S/MIME enabled e-mail client software.		

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	*De facto* standard from RSA Security, PKCS#7 syntax is widely used in S/MIME v2 (native support), S/MIME v3 or v4 (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.
Forward outlook	In secure e-mail, PKCS#7 v1.5 is supported in S/MIME v2 (native support) and S/MIME v3 or v4 (backward compatible). S/MIME, the dominant e-mail security standard, is based on CMS (RFC 5652). In file-based signing / encrypting applications, the migration from PKCS#7 to CMS (RFC 5652) is not noticeable. Therefore, PKCS #7 v1.5 will remain the standard for file-based cryptographic message syntax.
Version and rationale for version	Version 1.5 is a mature standard and is supported by the file-based signing / encrypting applications.

Standard 1 PKCS #7 v1.5 (RFC 2315)	
Limitations on the use of this standard	None.

Standard 2 S/MIME (Secure Multi-purpose Internet Mail Extensions) v3 or v4	
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 e-mail clients from Microsoft and Mozilla and has also been endorsed by other vendors that make messaging products.
Rationale for selection	S/MIME is a mature and well supported standard. S/MIME is undergoing further development and is likely to remain the dominant standard to secure e-mail.
Maturity	S/MIME v2 was published as an Informational RFC (RFC 2311 and 2312) in March 1998. S/MIME v3 was made an IETF standard (RFCs 2630, 2632 and 2633) in June 1999. S/MIME v3.1 was made an IETF standard (RFCs 3850 and 3851) in July 2004. S/MIME v3.2 was made an IETF standard (RFCs 5750 and 5751) in January 2010. CMS (RFC 5652) was published in September 2009, it can support a variety of architectures for certificate-based key management, such as the one defined by the PKIX (Public Key Infrastructure using X.509) working group. The latest version, S/MIME v4.0, was made an IETF standard (RFC 8551) in April 2019. S/MIME v3.2 has thus become obsolete. Support of SHA-512 in digest algorithm, and marked SHA-1 as historic..
Forward outlook	S/MIME is undergoing further development to incorporate support for new encryption standards and enhancements.
Version and rationale for version	S/MIME v3 or v4 are recommended. However, different mail products may implement different sets of S/MIME 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 functions that are not supported by the receiver's mail clients. Meanwhile, the S/MIME compatible mail clients (Microsoft Outlook / Outlook Express and Mozilla Thunderbird) have natively supported S/MIME for many years.
Limitations on the use of this standard	None.

Standard 3 PDF version 1.5, 1.6, 1.7 (ISO 32000-1), or 2.0 (ISO 32000-2:2020)	
Please refer to the area "Document file type for content publishing" for details on PDF	
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
CMS (RFC 5652)	Cryptographic Message Syntax, CMS (RFC 2630), is the first version of the CMS on the IETF standards track in 1999. It defines a standard to digitally sign, digest, authenticate or encrypt arbitrary messages. S/MIME version 3 is described in CMS RFC 2630 through RFC 2634 inclusive and RFC 5035. The CMS (RFC 5652) was published to advance the CMS along the standards maturity ladder in September 2009. Backward compatibility with earlier versions of the CMS (RFC 2630, RFC 3369 and RFC 3852) is preserved and the trend of CMS should be closely monitored.

Other candidate standards

Other Standard(s)	Description
None	

3.3.1.3 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 MOSS SPF DKIM	S/MIME v3 or v4 SPF (RFC 7208) DKIM (RFC 6376)	DMARC
Remarks: For electronic submissions via e-mail pursuant to the ETO, members of the public should use only those S/MIME enabled e-mail client software.		

Recommended standards

Standard 1 S/MIME (Secure Multi-purpose Internet Mail Extensions) v3 or v4
Please refer to the area "Attachment of digital signature to electronic documents received under ETO" for details on S/MIME.

Standard 2 Sender Policy Framework (SPF) (RFC 7208)	
Description	SPF prevents sender address forgery at domain level for improved authenticity of e-mail. Following SPF, mail domain owners can publish in the Domain Name System (DNS) a list of IP addresses or subnets that are authorised to send e-mail on behalf of the domain. Mail recipient server may then check against those DNS records whether an incoming e-mail message is sent from a server on an authorised subnet.
Rationale for selection	If a domain publishes an SPF record, forged e-mails pretending to be from that domain are more likely to be caught by spam filters of recipient side if it checks SPF record. Therefore, an SPF-publishing mail domain is less attractive to spammers and phishers attempting to forge e-mails. Such domain in turn will less likely be blacklisted by spam filters or Internet security service providers, ultimately facilitating legitimate e-mails from the domain to get delivered to their intended recipients. The propagation of SPF records relies on DNS and optionally DNSSEC, which is now gaining in popularity.
Maturity	SPF version 1.0 specification (RFC 4408) was published by the IETF in April 2006 to define an experimental protocol for the Internet community. In April 2014, RFC 7208 was published by the IETF, making RFC 4408 obsolete.
Forward outlook	The specification is subject to further developments.
Version and rationale for version	RFC 7208 is the current version of SPF.
Limitations on the use of this standard	None.

Standard 3 DomainKeys Identified Mail (DKIM) (RFC 6376)	
Description	DKIM validates a domain name identity of an e-mail message through cryptographic authentication. The e-mail's message together with its header is digitally signed with the domain private key in the sending mail server to produce a DKIM signature, which is then transmitted together with the e-mail. Recipient of the e-mail can verify this signature by querying DNS to retrieve the corresponding public key, and thereby verify that the e-mail was sent by the claimed domain and has not been tempered with during transmission.
Rationale for selection	DKIM is a method for associating a domain name to an e-mail message, thereby allowing the recipient to verify, for example, the organisation responsible for the message. The association is set up by means of a digital signature which can be validated by recipients. The digital signature makes use of asymmetric encryption technology and propagation of the corresponding public key relies on DNS and optionally DNSSEC, which is now gaining in popularity.
Maturity	DKIM signature was published in May 2007 (RFC 4871). A number of clarifications and conceptualisations were collected thereafter, and specified in RFC 5672 in August 2009, in the form of corrections to the existing specification. In September 2011, RFC 6376 was published by IETF, making RFC 4871 & 5672 obsolete.
Forward outlook	The specification is subject to further developments.
Version and rationale for version	RFC 6376 is the current version of DKIM.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
DMARC (RFC 7489)	The Domain-based Message Authentication, Reporting and Conformance (DMARC) is an e-mail authentication protocol jointly developed by the Return Path and a consortium of mailbox providers and security vendors. The objective of the DMARC is to provide greater assurance on the identity of the sender of an e-mail message, thus addressing the problem of e-mail phishing. The DMARC is designed with some DNS-based policy to allow a sender or domain owner to manage the behaviour of a receiver upon the receipt of new e-mail message. By communicating the policy to the receiver, the receiver will be instructed to authenticate the legitimacy of the sender's e-mail address against SPF and DKIM, and, in turn, quarantine or reject any suspiciously fraudulent e-mail if the authentication is failed. In addition, the DMARC also provides a way for the receiver to report back to the sender or domain owner the actions performed under the policy, in order to monitor and improve the protection from fraudulent e-mails. Some well-known e-mail providers that support DMARC include Google and Yahoo!, for example. In 2015, the IETF RFC Editor published the DMARC (RFC 7489) on the Independent Submission stream for informational purpose. RFC 7489 is currently in the process of being adopted as the official input to the IETF DMARC Working Group.

Other candidate standards

Other Standard(s)	Description
Pretty Good Privacy (PGP)	PGP is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991. 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. 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. PGP had been acquired by Symantec in 2010. Symantec no longer offers a freeware version of PGP. However, they do allow the public to download the source code for peer review.
Privacy Enhanced Mail (PEM)	PEM is a 1993 IETF proposal for securing e-mail using public-key cryptography. Although PEM became an IETF proposed standard it was never widely deployed or used.
MIME Object Security Services (MOSS)	MOSS is a protocol that uses the multipart/signed and multipart/encrypted framework to apply digital signature and encryption services to MIME objects. MOSS was never widely deployed or used.

3.3.1.4 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 specifies a process for encrypting data and representing the result in XML. • Decryption Transform for XML Signature specifies an XML Signature "decryption transform" that enables XML Signature applications to distinguish between those XML Encryption structures that were encrypted before signing (and must not be decrypted) and those that were encrypted after signing (and must be decrypted) for the signature to validate.
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. In April 2013, W3C published "XML Encryption Syntax and Processing version 1.1" as a W3C recommendation.
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	XML Encryption Syntax and Processing version 1.1 is the latest version published by W3C.
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	

3.3.1.5 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 Syntax and Processing	XML-Signature Syntax and Processing (RFC 3275) XML Signature Syntax and Processing v1.1	None

Recommended standards

Standard 1 XML Signature	
Description	XML Signatures provide *integrity*, *message authentication*, and/or *signer authentication* 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	Both XML-Signature Syntax and Processing standards (IETF RFC 3275 and W3C version 1.1) are formal recommendations and are supported by major software developers.
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 as well as an IETF Standard RFC 3275. In June 2008, W3C published XML Signature Syntax and Processing (Second Edition). The second edition added Canonical XML 1.1 as a required canonicalisation algorithm and recommended its use for inclusive canonicalisation. In April 2013, "XML Signature Syntax and Processing v1.1" has been reviewed by W3C Members, software developers, and other W3C groups and interested parties, and was endorsed by the Director of W3C as a W3C Recommendation.

Standard 1 XML Signature	
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. W3C published XML Signature Syntax and Processing v2.0 as a candidate recommendation on 24 January 2012 and a Working Group Note on XML Signature Syntax and Processing v2.0 was published on 23 July 2015.
Version and rationale for version	XML-Signature Syntax and Processing (RFC 3275) is the current IETF standard and XML Signature Syntax and Processing v1.1 is the latest version published by W3C.
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	

3.3.1.6 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 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.

Standard 1 Internet Protocol Security (IPsec)	
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. Support for IPsec has already been included in the Windows Server such as Windows 2008 Server.
Forward outlook	IPsec will remain as 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	

3.3.1.7 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
Transport Layer Security (TLS) protocol	TLS v1.2 or v1.3	
Remarks: None		

Recommended standards

Standard 1 Transport Layer Security (TLS) v1.2 or v1.3	
Description	TLS protocol is to provide privacy and data integrity between two communicating applications.
Rationale for selection	TLS v1.2 is (in use since 2008) and v1.3 (in use since 2018) are the current supported TLS versions for securing internet communications published by IETF and specified in RFC 5246 & 8446 respectively. With significant community involvement in the review, these two versions of TLS are widely adopted by the industry.. The latest version of major browsers and web servers support both TLS v1.2 and v1.3.
Maturity	TLS v1.2 was published as RFC 5246 in August 2008. It describes both generic extension mechanisms for the TLS handshake client and server hellos, and specific extensions using these generic mechanisms. Specifically, TLS v1.2 improved flexibility in particular negotiation of cryptographic algorithms and provided additional support of SHA2 series (SHA-256, SHA-384 and SHA-512) hashing algorithm. TLS v1.3 is the latest version formally approved by the IETF on 21 March 2018 and published as RFC 8446 in August 2018. TLS v1.3 comes with some important security and performance improvements when compared to its previous versions. It adopts newer and stronger encryption and hashing algorithms, reduces time to initiate handshakes and establish encryption channels between web browsers and servers. It also prevents the downgrade attack where an attacker makes a TLS server connect to a client with an older and vulnerable version of the protocol. According to the NIST Special Publication (SP) 800-52 Revision 2, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations", NIST requires that all government TLS servers and clients support TLS 1.2 configured with FIPS-based cipher suites and recommends that agencies develop migration plans to support TLS 1.3 by January 1, 2024. (https://csrc.nist.gov/News/2019/nist-publishes-sp-800-52-revision-2) Both TLS v1.2 and v1.3 are the minimum recommended versions for the use of TLS and are now widely adopted by the industry. They are supported by major browsers and web servers.
Forward outlook	The TLS Working Group, established in 1996, continues to work on the TLS protocol and related applications. On March 2021, the IETF has formally deprecated TLS v1.0 and v1.1 (https://datatracker.ietf.org/doc/html/rfc8996).
Version and rationale for version	TLS v1.2 and v1.3 are recommended as they are the versions with wider industry adoption.
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	

3.3.1.8 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
3DES AES Blowfish DES	AES	None
Remarks: 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.		

Recommended standards

Standard 1 Advanced Encryption Standard (AES)	
Description	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 is a standard accepted by the NIST and is widely accepted as the de facto standard in security-related applications.

Standard 1 Advanced Encryption Standard (AES)	
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 in November 2001 and became effective in May 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).
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
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.
DES	DES was developed in the early 1970s at IBM. 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. It is now considered to be insecure for many applications due to the 56-bit key size being too small. DES has been withdrawn as a standard by the NIST since July 2004.
3DES	3DES is a cipher suite based on the Data Encryption Standard (DES) developed by IBM in the early 1970s. 3DES has been a widely-used method of data encryption as the encrypted communication is re-encrypted twice to make it harder to crack. It belongs to the "symmetric" family of algorithms and supports a key length of 168 bits. A security analysis and practical demonstration of attacks on 3DES in several real-world protocols provided evidence that the collision attack on 3DES represents a serious security vulnerability for many common uses of these protocols. According to the National Institute of Standards and Technology (NIST) Special Publication 800-131A Rev.2, "Transitioning the Use of Cryptographic Algorithms and Key Lengths" published in 2019, the 3DES will be deprecated through December 2023. After December 2023, 3DES will be disallowed for encryption unless specifically allowed by other guidance. Decryption using 3DES is allowed for legacy use.

3.3.1.9 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 (RFC 5753)	RSA	Elliptic Curve Cryptography (ECC) (RFC 5753)

Recommended standards

Standard 1 RSA	
Description	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. There is a global industry trend of adopting stronger cryptographic algorithms and keys to protect against algorithm breaks and / or availability of more powerful computing techniques. Many certification authorities (CAs) and product vendors have acted on the global trend and RSA keys should use key lengths no shorter than 2048 bits. CA/Browser Forum was advised by the NIST to deprecate signing Digital Certificates that contained RSA Public Keys of 1024 bits after 31st December 2010 and to cease signing completely by 31st December 2013 . In August 2012, Microsoft released a security advisory about releasing Windows Update to block cryptographic keys that are less than 1024 bits long starting from October 2012. Starting from Mac OS X 10.6.8, certificates containing RSA keys less than 1024 bits are rejected.
Rationale for selection	RSA is the dominant asymmetric encryption scheme. The ISO (International Standards Organisation) 9796 standard lists RSA as a compatible cryptographic algorithm.
Maturity	The RSA system was first developed in 1997 and is thus mature and has been extensively tested.
Forward outlook	RSA is the dominant asymmetric encryption algorithm and will continue to be developed by RSA Security.
Version and rationale for version	Only one version of RSA exists.

Standard 1 RSA	
Limitations on the use of this standard	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. According to the NIST Special Publication 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST advised moving to 2048-bit RSA keys beyond 2013.

Emerging standards for future consideration

Emerging Standard(s)	Description
Elliptic curve cryptography (ECC) (RFC 5753)	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. The use of ECC in Cryptographic Message Syntax is in the Informational RFC 3278 published in April 2002. It was then obsoleted by RFC 5753 in January 2010. 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. 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. 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. 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. 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. When asymmetric key algorithm is used to protect classified data, 224-bit or more for the ECC encryption should be used.

Other candidate standards

Other Standard(s)	Description
None	

3.3.1.10 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
Remarks: The interacting parties should either agree before implementation on the algorithm to use or should enable some auto-negotiation mechanism.		

Recommended standards

Standard 1 DSA (Digital Signature Algorithm)	
Description	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. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. The DSA provides the capability to generate and verify signatures. NIST defines key sizes of 1024, 2048 and 3072 bits under NIST SP 800-57.
Rationale for selection	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.
Maturity	The Digital Signature Algorithm is a Federal Information Processing Standard (FIPS) issued on May 19,1994.
Forward outlook	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. 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.
Version and rationale for version	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
Limitations on the use of this standard	According to the NIST Special Publication 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST advised moving to 2048-bit DSA keys beyond 2013.

Standard 2 RSA for Digital Signatures	
Description	RSA for Digital Signatures is an alternative method for generating and checking digital signatures.
Rationale for selection	RSA for Digital Signatures is recognised by the NIST within the Digital Signature Standard as an alternative to DSA or ECDSA.

Standard 2 RSA for Digital Signatures	
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	According to the NIST Special Publication 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST advised moving to 2048-bit RSA keys beyond 2013.

Emerging standards for future consideration

Emerging Standard(s)	Description
ECDSA	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. 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). 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, started to offer multi-algorithm SSL certificates with new ECC (RFC 5753) and DSA options in addition to RSA for X.509 certificates. 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. 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. 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. 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. 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.

Other candidate standards

Other Standard(s)	Description
None	

3.3.1.11 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-256, SHA-384 and SHA-512	SHA-3

Recommended standards

Standard 1 SHA-256, SHA-384 and SHA-512	
Description	SHA-256, SHA-384 and SHA-512 are series of SHA hash functions that are alternative hashing functions in computing a condensed representation of electronic data (message).
Rationale for selection	The SHA-2 (SHA-256, SHA-384 and SHA-512) families are designed by the National Security Agency (NSA) and published by National Institute of Standards and Technology (NIST). They are approved hash algorithms for digital signature. With longer bits of message digest, SHA-2 is more secure against brute force collision and inversion attacks.
Maturity	SHA-256, SHA384 and SHA-512 were published in 2002 in FIPS PUB 180-2 and it is included in the RSA PKCS#1 v2.1 published in June 2002. Many commercial / open-source software have already supported the new hashing algorithms.
Forward outlook	SHA algorithms will continue to be reviewed by NIST. NIST has announced Keccak as the winner of the SHA-3 Cryptographic Hash Algorithm Competition on 2 October 2012. On 6 November 2015, NIST released Special Publication (SP) 800-131A Revision 1, which included among others the SHA-3 family hash functions (specified in FIPS 202) as an approved hash function. The adoption on the use of SHA-3 FIPS standard should be closely monitored.
Version and rationale for version	SHA-256, SHA-384 and SHA-512 are algorithmically similar algorithms that differ in the number of bits of their digest length. The number in these three algorithms' names denotes the bit length of the digest they produce.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
SHA-3	NIST published a Federal Register Notice, on 5 August 2015 to announce the publication of Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and a Revision of the Applicability Clause of Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard. FIPS 202 specifies the SHA-3 family of hash functions, as well as mechanisms for other cryptographic functions to be specified in the future.

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".
SHA-224	SHA-224 was published as an additional variant in the change notice for FIPS PUB 180-2 in February 2004. SHA-224 is a truncated version of SHA-256, computed with different initial values. Although SHA-224 is one of the hashing algorithms in the SHA-2 family, it is not widely supported in commercial / open source software when compared to other algorithms in the SHA-2 family.
SHA-1	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. According to the NIST Special Publication 800-131A Revision 1, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST advised moving from SHA-1 to SHA-2 beyond 2013 and SHA-1 is approved for digital signature verification for legacy-use. Migration to SHA-2 family is suggested. NIST's current policy on hash functions indicates that SHA-1 should not be used for generating digital signatures, generating time stamps and for other applications that require collision resistance. It may be used to verifying old digital signatures and time stamps, generating and verifying hash-based message authentication codes, key derivation functions and random bit/number generation. In 2017, the three major browser vendors Microsoft, Google, and Mozilla have rolled out updates to stop trusting certificates signed with SHA-1. Their browsers will show an untrusted warning message to website visitors. SHA-1 is no longer a creditable hash algorithm for digital signatures in the industry and for end users. In February 2017, a research paper was issued to demonstrate the first known instance of SHA-1 collision by producing two different PDF files with the same SHA-1 signature, affirming that the hashing protocol is no longer considered secure.

3.3.1.12 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 MyGovHK. 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 CMS (RFC 5652)	PKCS #7 v1.5 (RFC 2315)	CMS (RFC 5652)

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
CMS (RFC 5652)	Please refer to the area "Attachment of digital signature to electronic documents received under ETO" for details on CMS (RFC 5652).

Other candidate standards

Other Standard(s)	Description
None	

3.3.1.13 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
Online Certificate Status Protocol (OCSP) (RFC 6960)	Online Certificate Status Protocol (OCSP) (RFC 6960)	None

Recommended standards

Standard 1 Online Certificate Status Protocol (OCSP) (RFC 6960)	
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 6960 specifies a protocol useful in determining the current status of a digital certificate without requiring CRLs.
Rationale for selection	RFC 6960 is an IETF standard, widely adopted for on-line certificate status protocol.
Maturity	RFC 2560 is an IETF standard published in June 1999 and was then obsoleted by RFC 6960 in June 2013.
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.
Version and rationale for version	RFC 6960 is recommended as it started to have wider industry adoption.
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	

3.3.1.14 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 (RFC 4211)	PKCS #10 v1.7 (RFC 2986)	None

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	*De facto* 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.
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
None	

Other candidate standards

Other Standard(s)	Description
Certificate Request Message Format (CRMF) (RFC 4211)	The Internet X.509 Certificate Request Message Format (CRMF) is 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.

3.3.1.15 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 5280 (X.509 v3)	RFC 5280 (X.509 v3)	None

Recommended standards

Standard 1 RFC 5280 (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	Originally published as a proposed standard (RFC 2459) in January 1999 and subsequently revised as RFC 3280 in April 2002. In May 2008, IETF further revised the standard as RFC 5280, it is deemed to be generally stable.
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 5280 (X.509 v3) is the current standard for certificate profile. RFC 5280 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	

3.3.1.16 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 5280 (X.509 v2)	RFC 5280 (X.509 v2)	None

Recommended standards

Standard 1 RFC 5280 (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. In May 2008, IETF revised the standard as RFC 5280.
Rationale for selection	RFC 5280 (X.509 v2) is the established, and the only viable Internet standard for profiling X.509 CRLs. RFC 5280 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. In May 2008, IETF further revised the standard as RFC 5280, it is deemed to be generally stable.
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 5280 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	

3.3.1.17 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 v1.1	None

Recommended standards

Standard 1 PKCS#12 v1.1	
Description	PKCS #12 governs the format used for the export and import of personal identity information. RFC 7292 is an IETF standard published in July 2014. RFC 7292 represents a republication of PKCS #12 v1.1 from RSA Laboratories' Public Key Cryptography Standard (PKCS) series. By publishing this RFC, change control is transferred to the IETF.
Rationale for selection	*De facto* 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, v1.1 published in October 2012.
Forward outlook	Further development of PKCS standards occurs through mailing list discussions and workshops.
Version and rationale for version	PKCS #12 (Version 1.1) is recommended as it is still the version with wider industry adoption.
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	

3.3.1.18 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 /CNG PKCS #11 v3.0	PKCS #11 v2.11 Microsoft CryptoAPI /CNG	PKCS #11 v3.0
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, e-mail clients etc., and devices on which cryptographic operations are performed.
Rationale for selection	*De facto* 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/CNG	
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. CryptoAPI is the basis of Microsoft's Internet Security Framework. Starting from Windows Vista, the cryptographic provider of Microsoft was updated as Cryptographic API: Next Generation (CNG).
Rationale for selection	Mature standard. Required for supporting Microsoft products.
Maturity	CryptoAPI was introduced by Microsoft in 1996. Starting from Windows Vista, CryptoAPI was updated as CNG.
Forward outlook	It is likely that CryptoAPI/CNG will remain the dominant standard on Microsoft platforms, as an alternative to PKCS #11.

Standard 2 Microsoft CryptoAPI/CNG	
Version and rationale for version	Not applicable. Microsoft CryptoAPI/CNG is provided as part of the core platform SDK and is embedded within appropriate products.
Limitations on the use of this standard	Specific to Microsoft products.

Emerging standards for future consideration

Emerging Standard(s)	Description
PKCS #11 v3.0	PKCS #11 defines the interface between applications, such as Web browsers, e-mail clients etc., and devices on which cryptographic operations are performed. De facto standard from RSA Security, PKCS #11 is widely supported by the market leading browsers, software development kits, security tokens and smart card readers. 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. OASIS PKCS #11 v3.0 specification become approved OASIS standards on 15 June 2020. 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. PKCS #11 v2.11 is more widely adopted and it is suggested to keep the specification as the recommended one. When compared with the more widely adopted version, PKCS #11 v3.0 was approved by OASIS in Jun 2020. Although the industry has started its work to support this new specification, it is still not fully supported yet. Hence, it is suggested to include PKCS #11 v3.0 as an emerging standard and keep in view the implementation status in the industry in the near future.

Other candidate standards

Other Standard(s)	Description
None	

3.3.1.19 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	*De facto* 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	

3.3.1.20 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 WS-Federation ID-FF	SAML v1.1 or v2.0 WS-Federation v1.2	None

Recommended standards

Standard 1 Security Assertion Markup Language (SAML) v1.1 or v2.0	
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	SAML has the following advantages: **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. **Loose coupling of directories**. SAML does not require user information to be maintained and synchronised between directories. **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-customised user experience at each service while promoting privacy. **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. **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.
Maturity	SAML had been formulated as an 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. OASIS is now taking effort to the development of SAML v2.1. The envisaged SAML v2.1 would clean up the existing SAML v2.0 specifications and incorporate some of the extensions that have been developed over the years.

Standard 1 Security Assertion Markup Language (SAML) v1.1 or v2.0	
Version and rationale for version	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: • 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) A number of organisations (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.
Limitations on the use of this standard	None.

Standard 2 WS-Federation v1.2	
Description	WS-Federation is an overall effort from IBM and Microsoft to build a basic model for different security domains to federate. It is also backed by some IT major players, such as IBM, Microsoft, BEA, Verisign and RSA Security. According to the specification, the primary goal of the WS-Federation is to "enable federation of identity, attribute, authentication, and authorisation information.". WS-Federation is a building block that is used in conjunction with other Web service, transport, and application-specific protocols to accommodate a wide variety of security models. WS-SecurityPolicy, WS-Security, and WS-Trust are the bedrocks of the WS-Federation. WS-SecurityPolicy represents the security requirements and capabilities of Web services via assertions. WS-Trust introduces the Security Token Service (STS) for requesting and issuing the security tokens which are exchanged to authenticate principles and protect message / resources. WS-Security defines mechanisms for assuring message / resource authenticity, integrity and confidentiality through the use of security tokens.
Rationale for selection	WS-Federation v1.2 is the OASIS standard. It is recognised as one of the industry-wide standards for identity federation.
Maturity	In 2003, the initial draft of WS-Federation was published for public review and evaluation. The major version 1.0 of WS-Federation was approved in July of the same year. Release of WS-Federation v1.1 followed in December 2006. OASIS Web Services Federation (WSFED) Technical Committee announced and ratified WS-Federation v1.2 as an official OASIS standard in May 2009. It is observed that several products in the market implements WS-Federation for identity federation. Examples of the products include Cloud Federation Service of Radiant Logic, ADFS 2.0 of Microsoft, NetIQ Access Manager of NetIQ, OpenAM of ForgeRock, Oracle Federation Identity of Oracle, and Tivoli Federated Identity Manager of IBM.

Standard 2 WS-Federation v1.2	
Forward outlook	The specification is subject to further developments. The WSFED Technical Committee, established in 2007, continues to work on the specification.
Version and rationale for version	None.
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
Identity Federation Framework (ID-FF) v1.2	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: • Businesses to create new relationships with each other and to realise 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 personalisation, security and control over identity information. The Liberty Alliance (the Kantara Initiative now) had no intention to further enhance and develop ID-FF after the ID-FF v1.2 was released. ID-FF v1.2 was contributed to the OASIS in 2003 and was subsequently converged into SAML v2.0. SAML v2.0 is therefore functionally equivalent to the ID-FF v1.2. ID-FF v1.2 is no longer an emerging standard of this area.

3.3.1.21 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	

3.3.1.22 Cyber threat information sharing standards

Justification for inclusion and usage

The need for the exchange of standardised cyber threat information grows with increasing numbers of discovered exploits of cyber vulnerabilities and attacks. There has been a diverse array of initiatives to develop structured expressions and associated protocols for the trusted exchange of information concerning the vulnerabilities and attacks, and remediation measures. Through sharing of relevant cyber threat information among trusted parties, each sharing party can potentially gain a more accurate situational awareness of the threat landscape.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
STIX v1.2.1 or v2.0 or v2.1 TAXII v1.1.1 or v2.0 or v2.1 TLP v1.0 or v2.0	STIX v1.2.1 or v2.0 or v2.1 TAXII v1.1.1 or v2.0 or v2.1 TLP v2.0	None

Recommended standards

Standard 1 Structured Threat Information eXpression (STIX) v1.2.1 or v2.0 or v2.1	
Description	STIX (Structured Threat Information eXpression), under OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC), (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-stix) is a standardised XML programming language for conveying information, including observable, indicator, incident, tactics, techniques & procedures (TTP), exploit target, course of action (COA), campaign, and threat actor, about cyber security threats. STIX enables organisations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.
Rationale for selection	STIX v1.2.1 has been adopted by some common Information Sharing and Analysis Centres (ISAC) in USA such as Financial Services ISAC, National Health ISAC and Industrial Control System ISAC, and Hong Kong Association of Banks (HKAB) Cyber Intelligence Sharing Platform (CISP) in HKSAR to facilitate the exchange of cyber threat information among participating members in the respective industry sectors. Also, STIX is open source and is being implemented in many products and services. In addition, open source threat information feeds (e.g. VirusTotal and SANS Internet Storm Center) in STIX format are available for general use. STIX v2.0 has been significantly redesigned and, as a result, omits some of the objects and properties defined in STIX v1.2.1. STIX v2.1 has further enhanced to include new objects from STIX v2.0. The objects and features added for inclusion in STIX v2.1 represent an iterative approach to fulfilling basic consumer and producer requirements for CTI sharing.
Maturity	STIX v1.2.1 was published as an OASIS Committee Specification in May 2016 (https://www.oasis-open.org/standards#stix1.2.1). STIX v2.0 was published as an OASIS Committee Specification with version approved in July 2017. STIX v2.1 was published to replace STIX v2.0 as an OASIS Committee Specification with version approved in March 2020. (http://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html)
Forward outlook	The OASIS Cyber Threat Intelligence Technical Committee will be focusing on advancing STIX v2 and there will be no further revisions of STIX v1.2.1.
Version and rationale for version	STIX v2.0, v2.1 and v1.2.1 are the latest version published by OASIS CTI TC.
Limitations on the use of this standard	Interoperability between different implementations of the STIX specifications cannot be guaranteed. 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., deploy STIX 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 may arise.

Standard 2 Trusted Automated eXchange of Indicator Information (TAXII) v1.1.1 or v2.0 or v2.1	
Description	TAXII (Trusted Automated eXchange of Indicator Information), under OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC) (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-taxii), is a standard for exchanging standardised cyber threat information in a trusted manner. TAXII defines services, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber security threats.
Rationale for selection	TAXII defines a set of services and message exchanges that enables sharing of actionable cyber threat information across organisation and product/service boundaries. TAXII enables organisations to achieve situational awareness about emerging threats, and share the information they choose with the partners they choose all while using a common set of tools. TAXII v1.1.1 was designed to the TAXII application protocol to be hosted on top of multiple underlying transport protocols. Because the TAXII v1.1.1 protocol could not assume any particular underlying transport, this required that TAXII re-implements features and capabilities that were already provided by HTTP. In contrast, TAXII v2.0 is explicitly designed to serve as an application layer protocol on top of HTTPS and as such can rely on the full set of services provided by HTTPS implementations. In addition, TAXII v2.0 provides a RESTful interface to data and service which primarily uses HTTP as its underlying protocol. The latest TAXII v2.1 specification defines RESTful API and its resources along with the requirements for TAXII Client and Server implementations. TAXII protocol changes include the uses of HTTPS (HTTP over TLS) as the transport for all communications and removal of STIX media types and bundle with TAXII Envelope.
Maturity	TAXII v1.1.1 was published as an OASIS Committee Specification in May 2016 (http://docs.oasis-open.org/cti/taxii/v1.1.1/taxii-v1.1.1-part1-overview.html). TAXII v2.0 was published in October 2017 as an OASIS Committee Specification with version approved in July 2017. (http://docs.oasis-open.org/cti/taxii/v2.0/cs01/taxii-v2.0-cs01.html). TAXII v2.1 was published to replace TAXII v2.0 as an OASIS Committee Specification with version approved in January 2020. (https://docs.oasis-open.org/cti/taxii/v2.1/cs01/taxii-v2.1-cs01.html)
Forward outlook	The OASIS Cyber Threat Intelligence Technical Committee will be focusing on advancing TAXII v2 and there will be no further revisions of TAXII v1.1.1.
Version and rationale for version	TAXII v2.0, v2.1 and v1.1.1 are the latest version published by OASIS CTI TC.
Limitations on the use of this standard	Interoperability between different implementations of the TAXII specifications cannot be guaranteed. 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., deploy TAXII 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 may arise.

Standard 3 Traffic Light Protocol (TLP) v2.0	
Description	The Traffic Light Protocol (TLP), under the Forum of Incident Response and Security Teams (FIRST), was created in order to facilitate sharing of information (https://www.first.org/tlp). TLP is a set of designations used to ensure that information including cyber threat information is shared with the appropriate audience. TLP provides a schema for indicating when and how cyber threat information can be shared, and facilitating collaboration in a user community.
Rationale for selection	TLP was developed originally to encourage information sharing with and among public and private sector security professionals in the United Kingdom in the early 2000s. It is currently used by various types of Computer Security Incident Response Teams (CSIRT), operational trust communities, information sharing analysis organisations, government agencies, and private researchers, and has achieved "de facto" international standard status.
Maturity	TLP v2.0 is authoritative from August 2022 onwards (https://www.first.org/tlp/). TLP v1.0 was deprecated by FIRST in August 2022 (https://www.first.org/tlp/v1/).
Forward outlook	FIRST will continue to develop TLP.
Version and rationale for version	TLP version 2.0 is the latest version published by FIRST.
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
Traffic Light Protocol (TLP) v1.0	TLP v1.0 was the initial version of TLP standardised by FIRST. It was authoritative from 2017 until August of 2022, and may still be used until 31 December 2022. FIRST strongly recommends the use of TLP version 2.0.

3.3.1.23 Authentication and authorisation with distributed identity

Justification for inclusion and usage

The goal is to enable user authentication and authorisation with identity distributed over web services and cloud computing environment using authentication tokens such as USB tokens, mobiles, NFC-enabled keys, etc.

Relevant to submissions under ETO : No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
OpenID Connect OAuth FIDO Universal Authentication Framework (FIDO UAF) Client to Authenticator Protocols (CTAP) W3C Web Authentication (WebAuthn)	OpenID Connect 1.0 OAuth 2.0 FIDO Universal Authentication Framework (FIDO UAF) 1.1, 1.2 Client to Authenticator Protocols (CTAP) W3C Web Authentication (WebAuthn) Level 2	None

Remarks:

OpenID Connect (OIDC) supports federation protocol user identity from trusted third-party authentication authorities.

OAuth 2.0 allows a user to grant limited access to their resources on one site to another site, without having to expose their credentials.

FIDO UAF is an authentication protocol and allows online services to offer password-less and multi-factor authentication.

CTAP specifies a protocol for communication between a personal device with cryptographic capabilities (aka authenticator) and a host computer.

WebAuthn uses asymmetric cryptography with phishing protections built into the browser and platform for authenticating with websites.

Recommended standards

Standard 1 OpenID Connect 1.0	
Description	OpenID Connect is a suite of lightweight specifications that provide a framework for obtaining identity information of a user via Representational state transfer (REST) like APIs. The simplest deployment of OpenID Connect allows for clients of all types including browser-based, mobile, and javascript clients, to request and receive information about identities and currently authenticated sessions. The specification suite is extensible and also allows participants to optionally support encryption of identity data, discovery of the OpenID Provider, and advanced session management, including logout. OpenID Connect is a simple JavaScript Object Notation (JSON)/REST-based interoperable identity protocol built on top of the OAuth 2.0 family of specifications. OpenID Connect allows a user to authenticate to services (generically termed a Relying Party, or RP), such as mobile apps and Web-based applications, using an identity provided by another system (called the Identity Provider, IdP). Well known IdPs include Google, PayPal and Facebook. The OpenID Foundation finalised and officially launched the OpenID Connect v1.0 specification in February 2014. Examples of OpenID Connect deployments include Google, Microsoft, Ping Identity, Yahoo and PayPal.

Standard 1 OpenID Connect 1.0	
Rationale for selection	OpenID Connect can satisfy the Security Assertion Markup Language (SAML) use cases but with a simpler, JSON/REST based protocol. OpenID Connect was designed to also support native apps and mobile applications, whereas SAML was designed only for web-based applications. Benefits of OpenID Connect: • Improve and secure the exchange of information between parties for providing identity services • Fine-grained consent and authorisation
Maturity	There are already system-level APIs built into the mobile operating systems (iOS, Android) to provide OpenID Connect services. OpenID Connect can also be accessed by interacting with built-in system browser on mobile and desktop platforms.
Forward outlook	OpenID Connect standard is being developed by the OpenID working groups.
Version and rationale for version	OpenID Connect 1.0 is a mature version which is supported by various vendors for mobile devices, desktop operating systems, etc.
Limitations on the use of this standard	None

Standard 2 OAuth 2.0	
Description	OAuth provides a method for clients to access server resources on behalf of a resource owner (such as a different client or an end-user), it also provides a process for end-users to authorise third-party access to their server resources without sharing their credentials using user-agent redirections. OAuth specification is being developed within the IETF OAuth working group and is based on the OAuth Web Resource Authorization Protocol(WRAP) proposal. OAuth is an open standard for authorisation. The ongoing standardisation effort within the OAuth working group will focus on enhancing interoperability of OAuth deployments. (see http://tools.ietf.org/wg/oauth/charters) The OAuth 2.0 Authorisation Framework (RFC6749) and OAuth 2.0 Bearer Token Usage (RFC6750) specifications provide a general framework for third-party applications to obtain and use limited access to HTTP resources. OAuth Core v1.0, the main protocol, was finalised in December 2007 and v1.0a was issued on April 2009. The OAuth 2.0 Framework was published as RFC 6749 in October 2012. The best current practice of the OAuth 2.0 for Native Apps (RFC8252) was issued in October 2017. A growing number of social networking services promote OAuth2.0-based Single-Sign-On (SSO) services to the major social networks (Google, Facebook, Twitter, etc.) as the primary authentication method, over "traditional" e-mail confirmation type processes. Well known OAuth supporting providers include Google, Microsoft, Twitter and Facebook.
Rationale for selection	OAuth 2.0 is the industry-standard protocol for authorisation. OAuth 2.0 supersedes the work done on the original OAuth protocol created in 2007.

Standard 2 OAuth 2.0	
Maturity	OAuth 2.0 is a delegated authorisation framework for REST/APIs. It enables apps to obtain limited access (scopes) to a user's data without giving away a user's password. It decouples authentication from authorisation and supports multiple use cases addressing different device capabilities. OAuth 2.0 has gained rapid adoption across many websites including Facebook, Google and LinkedIn. OAuth libraries are available in a variety of languages such as Java, Python, PHP, Swift, etc.
Forward outlook	IETF OAuth Working Group will continue to develop OAuth specification and its extensions.
Version and rationale for version	OAuth 2.0 is a mature version supported by server-to-server apps, browser-based apps and mobile/native apps.
Limitations on the use of this standard	None

Standard 3 FIDO Universal Authentication Framework (FIDO UAF) 1.1, 1.2	
Description	The FIDO (Fast IDentity Online) Alliance, www.fidoalliance.org, was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users faced with creating and remembering multiple usernames and passwords. FIDO Authentication provides stronger, private, and easier to use when authenticating to online services. FIDO UAF 1.1 (Recommendation ITU-T X.1277) was first published in February 2017. A mobile standard providing authentication without passwords by using biometrics and other modalities to authenticate users to their local devices. FIDO UAF 1.2 was released in October 2020 and is backward compatible to FIDO UAF 1.1. Both FIDO UAF 1.1 and 1.2 are current FIDO Alliance authentication standards.
Rationale for selection	FIDO UAF 1.1 is an official ITU standard (ITU-T X.1277 Recommendations) to allow online services to offer password-less and multi-factor security.
Maturity	FIDO standards support a full range of authentication technologies, including biometrics such as fingerprint and iris scanners, voice and facial recognition, as well as further enabling existing solutions and communications standards, such as Trusted Platform Modules (TPM), USB Security Tokens, embedded Secure Elements (eSE), Smart Cards, Bluetooth Low Energy (BLE), and Near Field Communication (NFC).
Forward outlook	FIDO Working Groups will continue to develop FIDO specifications.
Version and rationale for version	FIDO UAF 1.1 and 1.2 supports users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.
Limitations on the use of this standard	None

Standard 4 Client to Authenticator Protocols (CTAP)	
Description	CTAP (Recommendation ITU-T X.1278) was approved on 29 November 2018. CTAP allows the use of external authenticators (FIDO Security Keys, mobile devices) for authentication on FIDO-enabled browsers and operating systems over USB, NFC, or BLE for a password-less, second-factor or multi-factor authentication experience.

Standard 4 Client to Authenticator Protocols (CTAP)	
Rationale for selection	CTAP is an official ITU standard (ITU-T X.1278 Recommendations). CTAP is being widely used in various industries such as the financial sector to provide strong online authentication based on public key cryptography and various user verification methods.
Maturity	CTAP (ITU-T X.1278 Recommendations) are under the responsibility of ITU's standardisation expert group for security, ITU-T Study Group 17. The CTAP protocol is already built into Windows 10, Android, Google Chrome, Mozilla Firefox, Microsoft Edge, as well as in preview by Apple Safari.
Forward outlook	FIDO Working Groups will continue to develop FIDO specifications. ITU-T Study Group 17 (SG17) coordinates security-related work across all ITU-T Study Groups and the FIDO Alliance.
Version and rationale for version	CTAP is the latest version of ITU-T X.1278 standard.
Limitations on the use of this standard	None

Standard 5 W3C Web Authentication (WebAuthn) Level 2	
Description	The Web Authentication API (also known as WebAuthn) is a specification written by the W3C and FIDO, with the participation of industry leaders such as Google, Mozilla, Microsoft, Apple and others. The API allows servers to register and authenticate users using public key cryptography instead of a password. The Web Authentication Working Group published WebAuthn Level 1 as a W3C Recommendation in March 2019. The updated version WebAuthn Level 2 was published in April 2021. It is a series of fixes and enhancements to the original specification. The focus for the Level 2 is to expand functionality for specific use cases. The Level 2 specification also describes the functional model for WebAuthn conformant authenticators, including their signature and attestation functionality.
Rationale for selection	WebAuthn is part of the FIDO Alliance's specifications and the FIDO Alliance runs certification programs to ensure compliance. The following benefits can be derived from adoption of WebAuthn Level: - Enterprise Attestation: supports controlled deployments within an enterprise where the organisation wishes to tie registrations to specific authenticators, allowing management functions such as tracking key distribution and usage. - Cross-Origin iFrame Support: maintains the integrity of the specification's single origin and allows for generating signatures in situations where authentication speed is required but limited by bandwidth, such as when using Bluetooth Low Energy and Near-Field Communication.
Maturity	WebAuthn is a standard for platforms and browsers for simple and strong authentication. It is a core component of the FIDO specifications, and is already supported in Google Chrome, Mozilla Firefox, Microsoft Edge and Apple Safari web browsers, as well as Windows 10 and Android platforms.
Forward outlook	The WebAuthn standard will continue to be monitored by Web Authentication Working Group.
Version and rationale for version	WebAuthn Level 2 is the latest version published by the W3C. It supersedes the WebAuthn Level 1 Recommendation with updates to improve usability and support.

Standard 5 W3C Web Authentication (WebAuthn) Level 2	
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	

3.3.1.24 Domain name system (DNS) security

Justification for inclusion and usage

Required to use cryptographic algorithms to protect DNS packets transmitted between DNS servers and clients from forgery, so as to enhance the trustworthiness of data in DNS.

Relevant to submissions under ETO：No

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
Domain Name System Security Extensions (DNSSEC)	Domain Name System Security Extensions (DNSSEC)	None

Recommended standards

Domain Name System Security Extensions (DNSSEC)	
Description	The Domain Name System Security Extensions (DNSSEC) is proposed by the IETF and are specified in RFC 4033. It provides resolvers (i.e. DNS clients) with the capability to authenticate the origin and assure the integrity of DNS data received. DNSSEC uses public key cryptography to verify the authenticity of a DNS record, by forming a "chain-of-trust" in which the chain normally starts from the DNS root server. All answers in DNSSEC are digitally signed (i.e. a digital signature together with the requested data). By validating the digital signature, the resolver is able to verify if the answer is from the authoritative DNS server and remains intact over the communication. Users are therefore protected from being redirected to malicious websites by spoofed DNS replies. Since July 2010, the root zone has been signed with a DNSSEC signature, providing a single trust anchor for the Domain Name System that can in turn be used to provide a trust anchor for other public key infrastructure. The Hong Kong Internet Registration Corporation Limited (HKIRC) announced the signing of DNSSEC for .hk and .香港 top-level domain name in May 2017.

Domain Name System Security Extensions (DNSSEC)	
Rationale for selection	The adoption of DNSSEC provides a new network security standard, which will not only reduce the time and economic loss for enterprises and users, but also help building Hong Kong network confidence among the public, tourists and even overseas investors, and ultimately enhance the position of Hong Kong's information technology across the region. DNSSEC is recommended by HKIRC and now with widely industry adoption in HK, such as "pcpd.org.hk" and "hkdnr.hk".
Maturity	Since the HKIRC officially announced the signed of DNSSEC for ".hk" and ".香港" domain names in May 2017, Hong Kong has over 60% DNSSEC total validation rate by APNIC Labs Measurements.
Forward outlook	ICANN is dedicated to ensure the stability of Internet and will work with HKIRC to popularize DNSSEC for a safer Internet environment for enterprises and the Internet community.
Version and rationale for version	With the use of DNSSEC, one can effectively reduce commercial fraud and identity theft, as well as security issues, such as unauthorised redirection of visitors to third party sites.
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 standardised 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). OASIS released the XACML version 2.0 as an approved OASIS standard in February 2005. XACML version 3.0 was announced and also ratified as an OASIS standard in January 2013. 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.

3.3.2.3 XML-based identity provisioning

Justification for inclusion and usage

Prepared for prospective support of automatic, effective and seamless user provisioning and de-provisioning, facilitating good identity management in the e-Government.

Standards for future consideration

Standard(s)	Description
SPML 1.0, 2.0	Service Provisioning Markup Language (SPML) is an open standard to define an interoperable XML-based request and response protocol for exchanging user, resource and service provisioning information between systems, as well as for describing operations to manage identity and access privilege in the target services. SPML is capable of supporting OASIS Web Service Security specification, XML Digital Signatures and XML Encryption. In SPML, a requesting authority (RA) sends well-formed SPML requests to a provisioning service provider (PSP). Web portal is an ordinary example of RA. The SPML requests are further processed by PSP. The PSP provides for corresponding provisioning actions, that RA requested, to provisioning service target. PSP finally replies the result of request to RA through SPML responses. In 2001, the OASIS Provisioning Service Technical Committee was constituted to design and formulate SPML. OASIS released the SPML 1.0 as an approved OASIS standard in November 2003. SPML 2.0 was announced and also ratified as an OASIS standard in April 2006. The SPML 2.0 defines some core operations including adding, modifying, deleting and querying objects (e.g. user accounts). In addition, the specification also provides password management and object suspension capabilities.
SCIM 1.1, 2.0	System for Cross-domain Identity Management (SCIM) specification is designed to manage user identity in cloud-based applications and services in a standardised way to enable interoperability, security, and scalability. The SCIM specification defines a unified and platform-neutral user schema and extension model for describing users and groups in XML and JSON formats. SCIM also provides standard API with rich identity management operations, such as adding, modifying, deleting and querying a single user identity or bulk user identities. The API operates across administrative domains over the Cloud through REST-based protocol. The specification aims to enable businesses to: • Simplify user management operation and at a lower cost. • Securely and effectively manage identities across cloud-based applications and services. • Improve interoperability and consistency of identity data. SCIM 1.1 was publicly released in July 2012. SCIM 2.0 was released as RFC7642 (Definitions, Overview, Concepts, and Requirements), RFC7643 (Core Schema) and RFC7644 (Protocol) under IETF in September 2015. SCIM 2.0 is not backward compatible to SCIM 1.1.

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 over TLS	SMTP (RFCs 5321, 5322) SMTP over TLS (RFC 3207)	None

Recommended standards

Standard 1 Simple Mail Transport Protocol (SMTP) (RFCs 5321 and 5322)	
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 5322 is complementary to RFC 5321, 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 5321 and 5322.
Limitations on the use of this standard	RFC 5321/5322 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. Such limitation in email body is addressed by Multipurpose Internet Mail Extensions (MIME) which enables the exchange of different types of data files. To support UTF-8 characters (RFC 3629) in email address or header information, one may refer to the SMTP extension as defined in RFC 6531.

Standard 2 SMTP over Transport Layer Security (TLS) (RFC 3207)	
Description	SMTP over TLS is to enhance the confidentiality, integrity and authenticity of Internet e-mail transmission on top of SMTP with hop-to-hop encryption, if both hops support. Once an SMTP connection between a sender mail server/client and the next-hop recipient SMTP server is established, the sender SMTP agent may optionally issue a STARTTLS command to initiate the TLS session. If the recipient SMTP agent accepts, both sides will then form an encrypted tunnel according to TLS. After that, e-mail(s) will be transmitted across in encrypted form.
Rationale for selection	Internet mail servers and clients commonly communicate over the Internet according to the SMTP protocol, but encryption is not part of SMTP protocol. This, for example, allows a third party, a.k.a. man-in-the-middle, to eavesdrop or alter the communications between the SMTP agents. Furthermore, there is often a desire for two SMTP agents to authenticate each other's identity. For example, an SMTP agent might only permit communications from other SMTP agents it knows, or it might act differently on e-mails received from an agent it does not know. TLS and its predecessor, SSL are cryptographic protocols that provide communication security for enhancing TCP connections, and depending on the cipher suites supported by both ends of the TCP connection, PKI digital certificates may be required. By increased security awareness in e-mail exchange in the Internet against any form of eavesdrops, the adoption of SMTP over TLS protocol is widely extending in market and now gaining in popularity.
Maturity	RFC 2487 on SMTP over TLS was released in January 1999, and was then obsoleted by RFC 3207 in February 2002.
Forward outlook	Nil.
Version and rationale for version	RFC 3207 is the current specification of SMTP service extension based on TLS.
Limitations on the use of this standard	Some products may not support this protocol.

Emerging standards for future consideration

Emerging Standard(s)	Description
None	

Other candidate standards

Other Standard(s)	Description
None	

3.4.1.2 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, 2049, 2231, 2387, 2392, 2557, 3676, 4289, 6838, 7303)	None

Recommended standards

Standard 1 Multipurpose Internet Mail Extensions (MIME) (RFCs 2045, 2046, 2047, 2049, 2231, 2387, 2392, 2557, 3676, 4289, 6838, 7303)	
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 5321 and 5322.
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 and 2049 published in 1996, RFC 4289 published in 2005 and RFC 6838 published in 2013. They were also complemented by RFC 2231 published in 1997, RFC 3676 published in 2004 and RFC 7303 published in 2014.
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, 2049, 2231, 2387, 2392, 2557, 3676, 4289, 6838, 7303.
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 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 2449 updated RFC 1939 in November 1998. RFC 5034 updated RFC 2449 in July 2007.
Forward outlook	POP3 will remain a dominant standard for remote mailbox access.
Version and rationale for version	Version 3 as defined in RFCs 1939, 2449 and 5034. RFC 1939 as a mature standard was introduced in May 1996, and was updated in November 1998 and July 2007.
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 replaced by RFC 2060 in 1996, which was then replaced by 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. The latest extension was published as RFC 6855 in 2013 to permit UTF-8 (RFC 3629) in headers, as described in "Internationalized Email Headers" (RFC 6532). It also adds a mechanism to support mailbox names using the UTF-8 charset.

Standard 2 Internet Message Access Protocol Version 4 (IMAP4) rev1	
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 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 WebSocket Protocol	HTTP/1.1 or HTTP/2	WebSocket Protocol HTTP/3

Recommended standards

Standard 1 HyperText Transfer Protocol HTTP/1.1 or HTTP/2	
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. HTTP/2 was published in May 2015. HTTP/2 can provide faster user experience for browsing, reduce the amount of bandwidth required, and make the use of secure connections easier. It is designed to allow a seamless switch between HTTP/1 and HTTP/2, with minimal changes to applications and APIs, while at the same time offering improved performance and better use of network resources. Web users largely will be able to benefit from the improvements offered by HTTP/2 without having to do anything different. Reference : https://www.ietf.org/blog/http2-approved/
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.

Standard 1 HyperText Transfer Protocol HTTP/1.1 or HTTP/2	
Maturity	HTTP has been in use by the World Wide Web global information initiative since 1990. HTTP/2 was published in May 2015 and is supported by the most current releases of common browsers like Edge, Safari, Firefox and Chrome.
Forward outlook	Both HTTP extensions and HTTP/1.1 are stable specifications. There is a growing trend of websites using HTTP/2. HTTP/2 is likely to have general use along with Web applications. (References : https://w3techs.com/technologies/details/ce-http2 https://httparchive.org/reports/state-of-the-web#h2)
Version and rationale for version	HTTP/1.1 is currently widely used. The latest update was published as RFC 9112 in June 2022. HTTP/2 was published in May 2015 and is supported by the most current releases of common browsers like Edge, Safari, Firefox and Chrome. HTTP/3 was published as a proposed standard in RFC 9114 in June 2022.
Limitations on the use of this standard	None.

Emerging standards for future consideration

Emerging Standard(s)	Description
WebSocket Protocol	The WebSocket Protocol is designed to supersede existing bidirectional communication technologies that use HTTP as a transport layer to benefit from existing infrastructure (proxies, filtering, authentication). Such technologies were implemented as trade-offs between efficiency and reliability because HTTP was not initially meant to be used for bidirectional communication. Conceptually, WebSocket is just a layer on top of TCP that: • adds a web origin-based security model for browsers; • adds an addressing and protocol naming mechanism to support multiple services on one port and multiple host names on one IP address; • layers a framing mechanism on top of TCP to get back to the IP packet mechanism that TCP is built on, but without length limits; and • includes an additional closing handshake in-band that is designed to work in the presence of proxies and other intermediaries. The WebSocket Protocol was standardised by the IETF as RFC 6455 in December 2011.
HTTP/3	HTTP/3 is the third major version of the Hypertext Transfer Protocol used to exchange information on the World Wide Web, complementing the widely-deployed HTTP/1.1 and HTTP/2. Unlike previous versions which relied on the well-established TCP (published in 1974),[1] HTTP/3 uses Quick UDP Internet Connections (QUIC), a multiplexed transport protocol built on UDP. In June 2022, IETF published HTTP/3 as a Proposed Standard in RFC 9114. (Ref: https://www.ietf.org/blog/http-updates/)

Other candidate standards

Other Standard(s)	Description
None	

3.4.1.5 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 replaced by RFC 1777 in March 1995, LDAP version 3 (RFC 2251) was introduced in 1997 and the latest specification was published as RFC 4511 in June 2006.
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	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). 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. There is limited activity in progressing the DAP specifications.

3.4.1.6 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 HKSAR (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 IDN	DNS IDN	None

Recommended standards

Standard 1 Domain Name System (DNS)	
Description	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. 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.
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 (For details, please refer to https://tools.ietf.org/html/rfc1034). RFC 1035 (For details, please refer to https://tools.ietf.org/html/rfc1035).
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	RFC 3490, RFC 3491 and RFC 3492 were standardised in 2003. RFC 3490 and RFC 3491 were replaced by RFC 5890 and RFC 5891 in 2010. The 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, RFC5890, RFC5891, RFC3492 and RFC3743, "Guidelines for the Implementation of Internationalized Domain Names" issued by ICANN.
Limitations on the use of this standard	The 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	

3.4.1.7 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 : Yes

Candidate Standard(s)	Recommended Standard(s)	Emerging Standard(s) for future consideration
FTP HTTP SFTP	FTP HTTP/1.1 or HTTP/2 SFTP	None
Remarks: 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. For server-to-client secure file transfer in a Web-based environment, the simplest way is to use HTTP over TLS to avoid having to install client-side software.		

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 TLS (ftps) can be used for secure file transfer between computers. It is an extension to FTP that adds security and authentication using TLS protocol, and it conforms to RFC2228. Products that support FTP over 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 or HTTP/2
Please refer to the area “Hypertext transfer protocol” for details on HTTP/1.1 or HTTP/2

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	As for SSH2, it was submitted as an Internet Engineering Task Force (IETF) draft in 1997. The IETF Secsh working group was responsible for the development of the SSH2 protocol (RFC 4251) also attempted to draft an extension of that standard for SFTP functionality. Internet Drafts were created that successively revised the SFTP protocol into new versions. The software industry began to implement various versions of the protocol before the drafts were standardised. As development work progressed, the scope of the SFTP project expanded to include file access and file management. Eventually, development stalled as some committee members began to view SFTP as a file system protocol, not just a file access or file transfer protocol, which places it beyond the purview of the working group. SFTP is not an Internet standard but it is still widely implemented and likely to remain as a popular secure file transfer protocol in the market.
Version and rationale for version	As of 2006, version 6 is the last revision to be produced by the IETF Secsh working group.
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
HTTP/3	Please refer to the area “Hypertext transfer protocol” for details on HTTP/3.

Other candidate standards

Other Standard(s)	Description
None	

3.4.1.8 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 IPv6	IPv4 IPv6	None

Remarks:

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.

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.

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 formalised 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) and RFC 2462 was replaced by RFC 4862 in 2007. 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.

Standard 2 Internet Protocol v6	
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	

3.4.1.9 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 UDP	TCP – preferred transport protocol over UDP UDP – where required e.g. to support particular protocols	None

Recommended standards

Standard 1 Transmission Control Protocol (TCP)	
Description	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. 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.
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.
Version and rationale for version	Currently only one version exists.

Standard 1 Transmission Control Protocol (TCP)	
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	

3.4.1.10 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 802.11ac IEEE 802.11ax Constrained Application Protocol (CoAP)	IEEE 802.11b IEEE 802.11g IEEE 802.11n IEEE 802.11ac IEEE 802.11ax	Constrained Application Protocol (CoAP)

Remarks:

Products of Wireless LAN with Wi-Fi Certification are recommended in order to ensure the interoperability between different manufacturers.

For all the IEEE 802.11 wireless LAN standards, the areas of access control, authentication, encryption, and data integrity are addressed by Wi-Fi Protected Access 2 (WPA2) and Wi-Fi Protected Access 3 (WPA3). For details, reference could be made to: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access and http://www.giac.org/paper/gsec/4214/wireless-security-ieee-80211-standards/106760

Recommended standards

Standard 1 IEEE 802.11 b/g	
Description	The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. There are numerous specifications in the family: from IEEE 802.11a to IEEE 802.11ai.
Rationale for selection	Both IEEE 802.11b and IEEE 802.11g are mature and widely adopted standards.
Maturity	IEEE 802.11 was accepted by the IEEE in 1997. IEEE 802.11b was ratified in 1999 and IEEE 802.11g was ratified in 2003.
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	IEEE 802.11b is widely adopted in market in all formats. 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.
Limitations on the use of this standard	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.

Standard 2 IEEE 802.11n	
Description	IEEE 802.11n defines mechanisms to provide significantly improved data rates and ranges for wireless local area networks (WLANs), it can be configured to operate in the 2.4 GHz or 5 GHz band. This new amendment to the IEEE 802.11 base standard is designed to help the data communications industry address the escalating demands placed on enterprise, home and public WLANs with the rise of higher-bandwidth file transfers and next-generation multimedia applications.
Rationale for selection	Draft version of IEEE 802.11n have been widely adopted in the market for several years before its ratification on 11 September 2009.
Maturity	IEEE 802.11 was accepted by the IEEE in 1997. IEEE 802.11n was ratified in 2009.
Forward outlook	As the IEEE 802.11 working group completes its work on IEEE 802.11n, the working group will begin developing standards targeting IMT-Advance reaching very high data rates at 1Gbps.
Version and rationale for version	IEEE 802.11n is backward compatible with IEEE 802.11b and IEEE 802.11g with higher throughput and will improve performance of wireless applications that are bandwidth demanding.
Limitations on the use of this standard	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 802.11n standard because it operates in the 2.4 GHz band or 5 GHz band, and the 5GHz band can be potentially used by WiMax or BRAN.

Standard 3 IEEE 802.11ac	
Description	IEEE 802.11ac is a wireless networking standard in the 802.11 family, developed in the IEEE Standards Association process, providing high-throughput wireless local area networks (WLANs) on the 5 GHz band. The specification is intended to achieve higher multi-user throughput in WLANs. The new amendment is intended to improve WLAN user experience by providing data rates up to 7 Gbps in the 5 GHz band. It adds channel bandwidths of 80 MHz and 160 MHz with both contiguous and non-contiguous 160 MHz channels for flexible channel assignment. It adds higher order modulation in the form of 256 quadrature amplitude modulation (QAM).
Rationale for selection	Draft version of IEEE 802.11ac has been adopted in the market since 2013 with related products like wireless routers, notebooks and smartphones. According to ABI Research, 802.11ac devices are expected to represent 45% of consumer Wi-Fi equipment shipments at the end of 2014.
Maturity	IEEE 802.11 was accepted by the IEEE in 1997. IEEE 802.11ac was ratified in January 2014.
Forward outlook	It is expected that 802.11ac will become the de-facto standard for 5-GHz equipment in a few years.
Version and rationale for version	IEEE 802.11ac is backward compatible with IEEE 802.11n with higher throughput and will improve performance of wireless applications that are bandwidth demanding.
Limitations on the use of this standard	802.11ac can be implemented only in 5 GHz. All the older technologies (e.g. 802.11b/g) that run predominantly in the 2.4 GHz band may need a separate radio/separate access points supporting 2.4 GHz to connect to the network.

Standard 4 IEEE 802.11ax	
Description	802.11ax is an IEEE standard for wireless local-area networks (WLANs) and the successor of 802.11ac. It is marketed as Wi-Fi 6 (2.4 GHz and 5 GHz) and Wi-Fi 6E (6 GHz) by the Wi-Fi Alliance. It is also known as High Efficiency Wi-Fi, for the overall improvements to Wi-Fi 6 clients under dense environments. It is designed to operate in license-exempt bands between 1 and 7.125 GHz, including the 2.4 and 5 GHz bands already in common use as well as the much wider 6 GHz band.
Rationale for selection	Products supporting 802.11ax are widely available in the market. The products are backward compatible with older Wi-Fi devices.
Maturity	802.11ax was marked as Wi-Fi 6 by the Wi-Fi Alliance in October 2018. 802.11ax-2021 was approved by IEEE in February 2021.
Forward outlook	It is expected that there will be a growth on the adoption of 802.11ax standard.
Version and rationale for version	802.11ax was marked as Wi-Fi 6 by the Wi-Fi Alliance in October 2018. Products supporting 802.11ax are widely available in the market.
Limitations on the use of this standard	None.

Other candidate standards

Other Standard(s)	Description
IEEE 802.11a	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. 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. Products of IEEE 802.11a are available in HKSAR market since the official regulation of 5GHz frequency band by the former OFTA in February 2003. OFTA has been replaced by OFCA since 1 April 2012. (See http://tel_archives.ofca.gov.hk/en/legislation/class-licence/wlan_guidelines.pdf http://www.coms-auth.hk/filemanager/common/licensing/Wireless_Local_Area_Network_Services_(Eng).pdf). 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. Major implementations of IEEE 802.11a are currently in the enterprise market. Products supporting IEEE 802.11a are relatively more expensive than IEEE 802.11 b/g and not widely adopted in low-end market.

Emerging standards for future consideration

Emerging Standard(s)	Description
CoAP	CoAP is a specialised web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things (IoT). The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation. It is also a specialised Internet Application Protocol for constrained

	devices that enables those constrained devices called "nodes" to communicate with the wider Internet using similar protocols. CoAP is designed for use between devices on the same constrained network (e.g., low-power, lossy networks), between devices and general nodes on the Internet, and between devices on different constrained networks both joined by an Internet. CoAP is also being used via other mechanisms, such as SMS on mobile communication networks.

3.4.1.11 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
WPA2 WPA3	WPA2 WPA3	None
Remarks: WPA2 provides a stronger encryption mechanism through AES, which is a requirement for some corporate and government users. WPA3 is backward compatible with current WPA2 devices and WPA2 devices will continue to interoperate and provide recognised security protection during the transition to WPA3 security in coming years.		

Recommended standards

Standard 1 Wi-Fi Protected Access 2 (WPA2)	
Description	The WPA specification used RC4 cipher. Subsequent standard WPA2 used AES cipher. WPA2 is better in security and is still a de-facto standard for wireless security. WPA has been retained in IF for some time because it takes time for hardware upgrade to support WPA2. Since March 2006, WPA2 has become a mandatory feature for all new Wi-Fi CERTIFIED products. Currently, WPA2 has been supported by all common hardware and it is appropriate to remove WPA from security point of view.
Rationale for selection	Nil
Maturity	Nil
Forward outlook	WPA2 standard will continue to be monitored by Wi-Fi Alliance.
Version and rationale for version	WPA2 is a mature version which is supported by mobile devices, desktop operating systems, and hardware network appliances from various vendors.
Limitations on the use of this standard	None.

Standard 2 Wi-Fi Protected Access 3 (WPA3)	
Description	The Wi-Fi Alliance announced WPA3 security in June 2018 as the next generation of Wi-Fi Protected Access security with enhancements on Wi-Fi protections in both personal and enterprise networks.
Rationale for selection	The WPA3 simplifies the authentication process and provides stronger encryption of sensitive data transmitted over the air.
Maturity	Products supporting WPA3 are widely available in the market (https://www.wi-fi.org/product-finder-results?keywords=wpa3&op=Search&form_build_id=form-OwXdjkIfrI-Ygf9qlJBApn2RI6fQ52aGEM2XnD5gJXI&form_id=wifi_cert_api_simple_search_form).
Forward outlook	WPA3 standard will continue to be monitored by Wi-Fi Alliance.
Version and rationale for version	Products supporting WPA3 are widely available in the market and continues to grow. While WPA3 is currently an optional certification for Wi-Fi CERTIFIED devices, it will become a required certification over time as market adoption grows (https://www.wi-fi.org/discover-wi-fi/security).
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	

3.4.2 Interoperability areas for future consideration – no apparent need yet

3.4.2.1 Audio-visual communications

Justification for inclusion and usage

For controlling communication sessions such as voice and video calls over Internet Protocol (IP).

Analysis

H.323 was defined by the ITU as a protocol designed for enterprise video conferencing. It borrowed much of the rich features defined in the previous generation H.320 systems that were designed for ISDN, but added to that functionality that was only possible on an IP network. It introduced an architecture that actually proved to be very robust and highly scalable, which then led to the widespread deployment of VoIP world-wide.

SIP was defined by the IETF as a protocol to enable end-to-end voice calls over the Internet. SIP has always been heralded as the protocol that will kill the PSTN and dominate the world, while at the same time it was touted as being a very simple, flexible protocol that anybody could employ in their products.

Standards for future consideration

Standard(s)	Description
Session Initiation Protocol (SIP)	The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions. Sessions may consist of one or several media streams. Other SIP applications include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer and online games.
H.323	H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.

3.4.2.2 Instant messaging and presence technology

Justification for inclusion and usage

For instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalised routing of XML data.

Analysis

Unlike most instant messaging protocols, XMPP uses an open systems approach of development and application, by which anyone may implement an XMPP service and interoperate with other organisations' implementations. Because XMPP is an open protocol, implementations can be developed using any software license; although many server, client, and library implementations are distributed as free

and open-source software, numerous freeware and commercial software implementations also exist.

Standards for future consideration

Standard(s)	Description
Extensible Messaging and Presence Protocol (XMPP)	XMPP uses an open systems approach of development and application, by which anyone may implement an XMPP service and interoperate with other organisations' implementations.

3.4.3 Interoperability areas for future consideration – standards not matured yet

3.4.3.1 Multicast for Layer 3 VPN

Justification for inclusion and usage

Defines implementation schemes used in a MPLS VPN (Multi-protocol Label Switching Virtual Private Network) for typical networking applications to travel from one VPN site to another VPN site.

The usage of multicast has been prevalent in software downloads and audio/video streaming applications. The volume of multicast traffic has been growing primarily based on the emergence of video-based applications.

Analysis

In order for IP multicast traffic within a BGP/MPLS IP VPN to travel from one VPN site to another, special protocols and procedures must be implemented by the related VPNs.

Standards for future consideration

Standard(s)	Description
Multicast in MPLS/BGP IP VPNs	Multi-protocol Label Switching / Border Gateway Protocol Virtual Private Network (MPLS/BGP VPN) is widely used as it provides flexible networking modes, excellent scalability, and convenient support for MPLS Quality of Service and MPLS Traffic Engineering. Multicast VPN is a technology to deploy the multicast service in an existing MPLS/BGP VPN. It transmits multicast data between private networks by encapsulating the original multicast packets. In February 2012, the Internet Engineering Task Force (IETF) has defined RFC 6513 ("Multicast in MPLS/BGP IP VPNs") to discuss the use of various BGP messages and procedures to provide MVPN support based on the deployed Multicast VPN solution of Cisco Systems. The RFC 6513 extends the RFC 4364 by specifying the necessary protocols and procedures to support IP multicast data or control traffic to travel from one VPN site to another.