

**Office of the
Government Chief Information Officer**

The HKSARG Interoperability Framework

[S18]

Version: 4.0

November 2005

The Government of the Hong Kong Special Administrative Region

COPYRIGHT NOTICE

© 2005 by the Government of the Hong Kong Special Administrative Region

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

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

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

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

Prepared By: Interoperability Framework Coordination Group

Doc. Effective Date: 1 March 2006

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
	Major updates to version 3.0 issued in November 2004 are as follows:		4.0	Nov 2005
1.	Add PDF v1.6 as a recommended standard in area “Document file type for receiving documents under ETO”	7-3		
2.	Introduce new interoperability area “Attachment of digital signature to electronic documents received under ETO” under the Information Access and Interchange Domain with PKCS #7 v1.5, S/MIME v3, and PDF v1.5 or 1.6 as recommended standard and Cryptographic Message Syntax (CMS) (RFC 3369) as emerging standard.	7-3, 7-10		
3.	Add OpenDocument 1.0 as a recommended standard in areas “Formatted document file type for collaborative editing”, “Presentation file type for collaborative editing”, and “Spreadsheet file type for collaborative editing”	7-3, 7-4		
4.	Introduce the new interoperability area “Content syndication” under the Information Access and Interchange Domain with RSS 1.0 or 2.0 as recommended standard and Atom as emerging standard.	7-7		
5.	Change the “Are the specifications relevant to submissions under ETO” column of the interoperability area “Cryptographic message syntax for file-based signing and encrypting” to “No” to cater for scenarios unrelated to the new area “Attachment of digital signature to electronic documents received under ETO”.	7-8		
6.	Promote RFC 3161 in area “Time stamping protocol” from emerging standard to recommended standard	7-9		
7.	Promote WPA as a recommended standard in area “Wireless LAN security” and revise the emerging standard from “IEEE 802.11i” to “WPA2 and IEEE 802.11i”	7-10, 7-11		
8.	Add WordProcessingML as an emerging standard for future consideration in area “Formatted document file type for collaborative editing”	7-11		

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
9.	Add SpreadsheetML as an emerging standard for future consideration in area “Spreadsheet file type for collaborative editing”	7-11		
10.	Add SHA-224, SHA-256, SHA-384 and SHA-512 under the 'emerging standards' for 'Hashing algorithms for digital signature'.	7-11		
11.	Add a remark against the area “Electronic Form” to provide guidelines for project teams in the selection of electronic form products	7-11		

TABLE OF CONTENTS

1.	EXECUTIVE SUMMARY	1-1
2.	PURPOSE AND STRUCTURE OF DOCUMENT	2-1
3.	OVERVIEW OF THE INTEROPERABILITY FRAMEWORK	3-1
3.1	THE NEED FOR AN INTEROPERABILITY FRAMEWORK.....	3-1
3.2	SCOPE OF THE INTEROPERABILITY FRAMEWORK	3-1
3.3	IMPACT OF THE INTEROPERABILITY FRAMEWORK	3-2
4.	MANAGEMENT OF THE INTEROPERABILITY FRAMEWORK.....	4-1
4.1	KEY REQUIREMENTS FOR MANAGEMENT MECHANISM	4-1
4.2	MANAGEMENT OF TECHNICAL SPECIFICATIONS	4-1
4.3	MANAGEMENT OF COMMON SCHEMAS	4-2
4.4	CHANGE MANAGEMENT	4-2
5.	COMPLIANCE.....	5-1
5.1	THE USE OF TECHNICAL SPECIFICATIONS AND COMMON SCHEMAS.....	5-1
5.2	COMPLIANCE POLICY	5-1
5.3	COMPLYING TO NEW VERSIONS OF THE INTEROPERABILITY FRAMEWORK	5-2
5.4	WHO NEEDS TO UNDERSTAND COMPLIANCE.....	5-3
5.5	RESPONSIBILITIES	5-3
5.6	PROCEDURES FOR EXEMPTION FROM COMPLIANCE	5-3
6.	PRINCIPLES UNDERLYING THE RECOMMENDATION OF TECHNICAL STANDARDS.....	6-1
6.1	PRINCIPLES TO BE OBSERVED BY PROJECT TEAMS WITH REGARD TO THE USE OF THE IF TECHNICAL STANDARDS.....	6-1
6.2	PRINCIPLES FOR INCLUDING INTEROPERABILITY AREAS UNDER THE IF.....	6-2
6.3	PRINCIPLES FOR SELECTING TECHNICAL STANDARDS UNDER THE IF....	6-3
7.	SPECIFICATIONS UNDER THE INTEROPERABILITY FRAMEWORK	7-1
7.1	OVERVIEW	7-1
7.2	APPLICATION INTEGRATION DOMAIN.....	7-2
7.3	INFORMATION ACCESS AND INTERCHANGE DOMAIN	7-2
7.4	SECURITY DOMAIN	7-8
7.5	INTERCONNECTION DOMAIN	7-9
7.6	OTHER SPECIFICATIONS UNDER OBSERVATION	7-10
8.	GOVERNMENT NETWORK ARCHITECTURE.....	8-1
8.1	OVERVIEW	8-1
8.2	MAJOR COMPONENTS OF THE GNA	8-1
8.3	COMPLIANCE AND ADOPTION OF THE GNA.....	8-2
8.4	NETWORK ARCHITECTURE	8-2
8.5	NETWORKING PROTOCOLS CURRENTLY SUPPORTED BY THE GNET	8-3
9.	ABBREVIATIONS AND ACRONYMS.....	9-1

1. EXECUTIVE SUMMARY

The Interoperability Framework (IF) supports the Government's strategy of providing client-centric joined-up services by facilitating the interoperability of technical systems between Government departments, as well as between Government systems and systems used by the public (including citizens and businesses).

The IF defines a collection of specifications aimed at facilitating the interoperability of Government systems and services. By bringing together the relevant specifications under an overall framework, IT management and developers can have a single point of reference when there is a need to identify the required interoperability specifications that should be followed for a specific project. By adopting these interoperability specifications, system designers can ensure interoperability between systems while at the same time enjoy the flexibility to select different hardware, and systems and application software to implement solutions.

The framework applies to both Government to Government interactions and Government to public interactions. It has no binding whatsoever on electronic interactions among members of the public (including businesses) themselves.

All new e-Government infrastructure systems, new Government to public (including businesses) systems, and new inter-Bureau and Department (B/D) systems must be developed based on the IF.

It is strongly recommended that all other new systems conform to the IF, as appropriate.

For existing systems, given the diversity of current platforms and systems, conformance to certain specifications may not be readily achieved. Existing systems are required to consider conformance to the IF only when there is a new requirement for government to public integration or inter-B/D integration, and only in respect of the modifications that specifically relate to external interfaces. Migration to the IF must be considered when a major functional change is being performed. In either case, connection or changes to existing systems are required to conform to the IF only when it is financially and functionally prudent to introduce compliance with the IF.

The development of an IF for e-Government is a long-term, ongoing strategy that must be continually reviewed and updated. Given the emergence of new business requirements and the pace of technological advancement, there are likely to be frequent changes to the specifications. The technical specifications under the IF will be reviewed every 6 to 12 months.

2. PURPOSE AND STRUCTURE OF DOCUMENT

This document describes the IF for the Government of the Hong Kong Special Administrative Region (HKSARG).

The information is arranged as follows:

- Section 3 provides an overview of the IF, including its objectives, and scope;
- Section 4 covers the management of the IF, including terms of reference for the governance bodies, membership criteria, and change management issues;
- Section 5 describes IF compliance, including compliance policy, responsibilities and procedures for exemption;
- Section 6 includes the principles underlying the recommendation of the IF technical standards;
- Section 7 lists the technical specifications selected for the identified interoperability areas. It also provides a list of the specifications under the IF;
- Section 8 describes the Government Network Architecture;
- Section 9 lists the abbreviations and acronyms used in this document.

Feedback on this report is welcomed, and comments may be addressed to:

The Interoperability Framework Coordination Group (IFCG)
Office of the Government Chief Information Officer

Email: ifcg@ogcio.gov.hk

3. OVERVIEW OF THE INTEROPERABILITY FRAMEWORK

3.1 THE NEED FOR AN INTEROPERABILITY FRAMEWORK

The development of the e-Government initiative is an on-going process of improving Government productivity and its provision of services to the public, enabled by technology.

A key business objective of current e-Government initiatives is to provide client-centric joined-up government services to the public, which requires the Government to be presented as a single organisation with the seamless flow of information, within legal bounds, across individual bureaux and departments (B/Ds) as necessary. An IF is essential to support the flow of information and to improve the coherence of information systems maintained by individual B/Ds.

The IF aims to define the set of specifications to facilitate Government systems to communicate and interoperate with other systems, both within Government and external to Government, efficiently and effectively. In addition, the IF promotes and fosters the adoption of eXtensible Markup Language (XML) to enable the exchange of data between applications.

In defining the HKSARG IF, we have studied international best practices, including the technical architecture and interoperability framework of other governments.

3.2 SCOPE OF THE INTEROPERABILITY FRAMEWORK

A major area where the IF is applied is to facilitate two information systems to interact to fulfill some business functions. To enable two information systems to interoperate, they have to be implemented based upon a mutually agreed set of specifications covering both the **business aspects** (e.g. how the business activities of one party interact with those of its business partners, what the legal consequences of such interactions are, what information needs to be sent from one party to another, the semantics behind the exchanged information, etc.) and the **technical aspects** (e.g. what protocol and message format should be used to send information from one party to another).

The IF helps the two parties to work out these specifications more effectively. It covers:

- A set of technical standards and data standards that help define the interface across different systems;
- Guidelines for project teams to work out some of the business-oriented specifications, where it is feasible to provide guidelines in that area; and
- Other standards documents that define infrastructure architecture, conventions and procedures.

The technical standards are listed in Section 7 of this document. The data standards are being progressively developed in the form of Common Schemas. The Common

Schemas define the information model of data elements that are often used in e-government applications; they serve as reusable components for composing project-defined data specifications.

To help B/Ds work out their information exchange specifications (project-defined schemas) more effectively, the XML Co-ordination Group has developed an XML Schema Design and Management Guide. The Guide provides a business information modeling methodology to help B/Ds model business documents and to translate information models into XML. The Guide also provides a framework for the development and use of Common Schemas. This Guide is published under the IF document library.

Infrastructure architecture, conventions and procedures specifications supplement the technical standards and data standards to facilitate interoperability. For example, the “LAN Addressing and Naming Standards” should be followed when B/Ds connect to common services¹, such as the Central Internet Gateway (CIG) and the Government Communication Network (GCN).

The infrastructure architecture specifications include the Government Network Architecture (GNA), which describes the overall network architecture. It defines the organisation and the relationship of the IT infrastructure components within Government. These components include Departmental Networks (DNs), Common Services (CSs) and the Government Backbone Network (GNET). Please refer to section 8 for a description of the GNA.

Specifications under the IF are published on the ‘IT in Government Information Station’ (ITG InfoStation) homepage² on the Government-wide Intranet. B/Ds should refer to these when implementing e-Government services. IF specifications relevant to the public are also published on the Internet³.

By bringing together the relevant specifications under an overall framework, IT management and developers can have a single point of reference when there is a need to identify the required interoperability specifications that should be followed for a specific project. By adopting these interoperability specifications, system designers can ensure interoperability between systems while at the same time having the flexibility to select different hardware, and systems and application software to implement solutions.

3.3 IMPACT OF THE INTEROPERABILITY FRAMEWORK

The framework applies to both Government to Government interactions and Government to public interactions. It has no binding whatsoever on electronic interactions between members of the public (including organisations) themselves.

¹ With regard to the use of common services, B/Ds may refer to the ‘IT in Government Information Station’ (ITG InfoStation) homepage on the Government-wide Intranet for more information.

² <http://itginfo.ccgo.hksarg/content/if/index.htm>

³ <http://www.ogcio.gov.hk/eng/infra/eif.htm>

Nevertheless, when members of the public build computer systems to interact with Government systems in the future, or when members of the public communicate with the Government electronically, the IF can provide the necessary specifications to enable effective interactions and communications between the private sector and the Government.

Internal Government B/Ds will feel the greatest impact of the IF. In the long term, the standards-based approach of the framework is intended to speed up the development of interoperating systems in B/Ds, for example, by reducing the amount of negotiation required for multiple parties to agree common specifications, allowing B/Ds to focus on the provision of value-added services. In the short to medium term, however, the impact of change resulting from compliance with the IF specifications might mean extra effort and cost. For example, it may be necessary to invest in XML-enabled middleware to integrate systems.

Due consideration has been given in the selection of technical specifications to technology, market trends, industry best practice and the current use of IT in Government in order to minimise the impact on B/Ds.

The impact of the Framework on external parties (citizens and businesses) will be less marked for a number of reasons:

- The principles used to select specifications for the IF have taken into account the availability of compliant solutions in the market, i.e. compliant solutions are readily available to the general public;
- Systems interfaces and access functionality will, particularly in the case of the public, be through browser-based systems and Internet technologies;
- Business-specific specifications will be determined with the help and agreement of the business sector itself.

4. MANAGEMENT OF THE INTEROPERABILITY FRAMEWORK

4.1 KEY REQUIREMENTS FOR MANAGEMENT MECHANISM

Appropriate management mechanisms are required to develop and manage the Common Schemas used within Government, as well as to ensure prompt review and update of the set of specifications that comprise the IF. These management mechanisms share several key requirements:

- They have to be sufficiently flexible to address the changes within the respective subject areas, such as technology changes;
- They have to address the fact that certain aspects, such as business specific conventions or technical specifications, would be more effectively owned and managed by business domain experts or dedicated specialist groups rather than under a common ownership; and
- Future changes to specifications could have profound impact not only on the Government, but also on individuals and organisations that need to interact with the Government. As such, there is a need for an effective consultation mechanism that allows the views from within the Government and the public to be channelled to the specialist groups responsible for managing the respective subject areas.

The overall IF, including the technical specifications, is managed by the **Interoperability Framework Co-ordination Group (IFCG)** and the management of Common Schemas is overseen by the **XML Co-ordination Group (XMLCG)**. The management mechanisms are described in the remainder of this section.

In addition, specialist groups in some B/Ds are taking the lead in developing interoperability standards for their respective industries (e.g. Computer-Aided-Drafting Standard for Works Projects, Common Spatial Units for Planning, Lands and Public Works Data). The IFCG will keep in close contact with these specialist groups and include relevant industry specific standards documents in the IF document library.

4.2 MANAGEMENT OF TECHNICAL SPECIFICATIONS

The overall IF, including the technical specifications, is managed by the Interoperability Framework Co-ordination Group (IFCG).

The Terms of Reference of the IFCG are:

- To advise the Government Chief Information Officer on the ongoing development and management of the Interoperability Framework;
- To co-ordinate the update of the Interoperability Framework to reflect technology advancement and application requirements;
- To monitor the effectiveness of the Interoperability Framework and suggest necessary enhancements;
- To promote and facilitate the adoption of the Interoperability Framework.

The IFCG comprises senior officers responsible for IT management in B/Ds, and may in future also include representatives from external organisations and experts in the field. Since the framework is designed to support future e-Government services, the IFCG is led primarily by the Office of the Government Chief Information Officer (OGCIO).

Specialist groups in the OGCIO, in turn, advise the IFCG on specific technical areas (e.g. the security specialists give advice on the security-related specifications).

The IFCG assigns individual specialist groups to lead the efforts in reviewing and recommending changes to specifications. The Government may adopt new specifications in the future. In this case, the IFCG will assign any new areas to the specialist groups, and where necessary establish additional specialist groups to advise on these new areas.

4.3 MANAGEMENT OF COMMON SCHEMAS

The framework for managing Common Schemas is specified in Part III of the XML Schema Design and Management Guide. Basically, a request for creating or changing a Common Schema would have to go through a consensus making process involving all interested B/Ds before the Common Schema would be registered. The XML Co-ordination Group (XMLCG) oversees the Common Schema management process. The XMLCG also develops pragmatic strategies to facilitate the effective adoption of XML in the HKSARG.

The Terms of Reference of the XMLCG are:

- To advise on strategies to facilitate the adoption of XML in the HKSARG;
- To advise on and facilitate the development of policies, guidelines and procedures to support the development and management of XML schemas for e-Government services;
- To advise on and facilitate the development and management of XML schemas for e-Government services; and
- To facilitate the sharing of experience in the use and implementation of XML.

The XMLCG reports to the Government Chief Information Officer and consists of experienced XML adopters in the public or private sector.

4.4 CHANGE MANAGEMENT

The IF specification documents are published on the ITG InfoStation homepage on the Government-wide Intranet. The IF specifications relevant to the public are also published on the Internet.

B/Ds or members of the public may request changes to the overall IF, including the technical specifications, by sending their change requests to the IFCG (email: ifcg@ogcio.gov.hk).

The development of an IF for e-Government is a long-term, ongoing strategy that must be continually reviewed and updated. Given the emergence of new business requirements and the pace of technological advancement, there are likely to be frequent changes to the technical standards. In order to facilitate the change cycle, the technical standards will be reviewed every 6 to 12 months.

B/Ds and relevant stakeholders will be consulted before changes to the specifications are finalised. Consultation will be conducted electronically via the ITG InfoStation and the Internet where relevant.

5. COMPLIANCE

5.1 THE USE OF TECHNICAL SPECIFICATIONS AND COMMON SCHEMAS

Compliance with the IF is mandatory for all B/Ds, as appropriate, when exchanging information between, or interoperating with other B/Ds, citizens and businesses.

Compliance means B/Ds are required to use those technical specifications and matured Common Schemas, plus the guidelines, infrastructure architecture, conventions and procedures specifications listed in the IF document library, where these exist and where applicable. For new systems where existing technical specifications or Common Schemas do not address interoperability requirements, a request for change should be raised.

The IF defines the basic collection of specifications that system interfaces must comply with when those systems interact with the systems of other B/Ds or the public. Individual systems may, subject to business requirement, offer additional system interfaces on top of the basic requirement.

5.2 COMPLIANCE POLICY

All new e-Government infrastructure systems, new government to public (including businesses) systems, and new inter-B/D systems must be developed based on the IF.

It is strongly recommended that all other new systems (for example, intra-B/D systems) conform to the IF, as appropriate, to minimise the impact of future requirements to interoperate.

For existing systems, given the diversity of current platforms and systems, conformance to certain specifications may not be readily achieved. Existing systems are required to consider conformance to the IF only when there is a new requirement⁴ for government to public integration or inter-B/D integration, and only in respect of the modifications that specifically relate to external interfaces. Migration to the IF must be considered when a major functional change is being performed. In either case, while the new business or functional requirements must be met in an effective manner, connection or changes to existing systems are required to conform to the IF only when it is financially and functionally prudent to introduce compliance with the IF.

Outsourcing of Government systems implementation is a growing trend. The IF will be applicable not only to systems owned by the Government but also those developed or implemented by vendors under the conditions that such systems connect to or have the potential to connect to other Government systems or systems of external parties. In such cases, compliance with the IF must be specified as a requirement for the interface component(s).

⁴ One example of such new requirement is a new format and manner requirement for electronic submission under the Electronic Transactions Ordinance (ETO).

Although the recommended specifications are provided only as a reference to the general public, the IF reflects the Government's preferred mechanism for communication with the public.

There are, however, a number of specifications intended to be relevant to electronic submissions under the Electronic Transactions Ordinance (ETO). These specifications will be promulgated, together with any additional requirements or relaxation necessary to fulfil B/Ds' operational need, through government notices to be published in relation to Format and Manner Requirements specified by the Permanent Secretary for Commerce, Industry and Technology (Communications and Technology) pursuant to the ETO.

Upon the publication of a new version of the IF, consequential amendments to the Format and Manner Requirements, where necessary, will be specified by the Permanent Secretary and published through government notices on or after the effective date of that version of the IF. Therefore, B/Ds should ensure that their computer systems designated to accept electronic submissions from the public can support the relevant IF specifications before that version of the IF becomes effective.

5.3 COMPLYING TO NEW VERSIONS OF THE INTEROPERABILITY FRAMEWORK

New integration projects should comply with the version of the IF effective on the date the project seeks endorsement for project implementation. If the version of the IF has changed since the system was designed and the changes impact on the system design, then the project team is required to conduct a cost/benefit analysis to assess the feasibility of changing the system design to comply with the updated IF.

The same principle applies when the IF is updated during project implementation and the updated version impacts on that implementation. A cost/benefit analysis must be undertaken to assess the feasibility of changing the system specification to comply with the updated IF.

In certain circumstances, the benefits of compliance with the updated IF may outweigh the costs in which case it would be appropriate to adapt the design. In other circumstances it may not be feasible for a system under development to adapt its design to comply with the new version of the IF due to budget, time, and contractual constraints, in which case it would not be appropriate to comply with the updated IF. The objective of the cost/benefit analysis is to ensure that project teams assess the situation in the event that the new version of the IF impacts on their project under development. The result of the cost/benefit analysis should be endorsed by the Head of the IT Management Unit (or its equivalent).

Existing procedures should be followed to seek additional funding in the event that the cost/benefit analysis determines the system should comply with a later version of the IF and additional cost will be incurred.

5.4 WHO NEEDS TO UNDERSTAND COMPLIANCE

An understanding of the IF and requirements for compliance should be as broad as possible across Government. In particular, the following parties will need a strong understanding of the issues:

- E-Business co-ordinators within B/Ds – need to understand the IF at a high level and be aware that any systems involving interaction between B/Ds or between B/Ds and the public are required to comply with the IF at external system interfaces;
- Head of the IT Management Units (or its equivalent) in B/Ds – need a thorough understanding of the IF and the compliance policy to ensure appropriate compliance and to justify exemption if necessary;
- B/D IT project managers – need a thorough understanding of the IF to ensure projects achieve compliance as directed by the Head of the IT Management Unit (or its equivalent). As soon as the need for exemptions are identified, project managers are required to justify them in writing for approval by the Head of the IT Management Unit (for B/Ds without an IT Management Unit, the project manager should seek exemption approval from the Departmental Liaison Officer (DLO) from OGCI), and report approved exemptions to the IFCG. They must also report on compliance with the IF when completing post-implementation departmental returns;
- Application developers – need a thorough understanding of the IF to adopt relevant specifications as directed during system design and development;
- Project approval authorities – need to understand the IF compliance policy and ensure that IF compliance is taken into account during the project approval process;
- Government IT suppliers: including technology, consultancy, and outsourcing providers – need a thorough understanding of the IF to ensure that solutions proposed to Government comply with the IF where appropriate;
- Project auditors and reviewers – need a high-level understanding of the IF to ensure that IF compliance is taken into account during the audit and review of projects.

5.5 RESPONSIBILITIES

Compliance will be self-regulated by individual B/Ds. Relevant stakeholders (e.g. project managers and application developers) should take individual responsibility for compliance.

Issues concerned with compliance with the IF should be raised with the IFCG. The Standing Office supporting the IFCG will provide information and answers to any queries raised by B/Ds on IF compliance.

5.6 PROCEDURES FOR EXEMPTION FROM COMPLIANCE

Where a system interface is applicable for IF conformance, should any IT project manager consider that there is a need to build the system's external interface using specifications that do not conform with those recommended in the IF, he / she is

required to seek compliance exemption approval from the Head of the concerned IT Management Unit with justifications in writing. For B/Ds without an IT Management Unit, the project manager should seek exemption approval from their DLO from OGCIO.

The Head of the IT Management Unit (or the DLO) will use their professional judgement in approving exemption requests, and approval to exemptions has to be made explicitly in writing. The IFCG should be consulted in the event of uncertainty.

Although compliance to the IF is governed on a self-regulatory basis, exemptions approved by the Heads of the IT Management Units (or the DLO) need to be reported to the IFCG within 2 weeks of approval if those exemptions are related to the external system interface of:

- new infrastructural systems (e.g. a shared transaction portal);
- new Government to public systems;
- new inter-B/D systems.

Such reports will help the IFCG assess and improve as soon as practicable the applicability and effectiveness of the IF, with a view to developing a sustainable and pragmatic framework useful to B/Ds.

In addition, upon receipt of such reports, the Standing Office supporting the IFCG will work with the specialist groups to assess the impact of the exemption and take actions to improve the situation, where necessary.

Under certain circumstances, B/Ds may be required to seek approval for exemption from compliance because their systems need to comply with industry-specific technical standards (such as those issued by the International Civil Aviation Organisation) when they exchange information with some of their business partners. Under such circumstances, project teams of that B/D only need to make one single exemption request to cover all subsequent identically justified exemptions from that technical standard.

In the case of a joined-up project steered by a cross-departmental Project Steering Committee (PSC) which comprises a Member with technical background (the Senior Technical role in PRINCE terminology), then only one exemption report needs to be filed to the IFCG provided that the exemption report has:

- listed all the affected projects in all concerned B/Ds; and
- declared that this exemption request has been endorsed by the cross-departmental PSC.

There are circumstances where IF compliance should be considered but need not be mandated. In such circumstances, project teams are given the flexibility to assess various considerations and design the most suitable interface between systems. Given that the appropriateness of the interface design will undergo the project's quality assurance mechanism which will take IF conformance and other project specific

requirements into consideration, deviation from the IF in such circumstances need not be reported as an exemption. These circumstances include:

- connection or changes to existing systems – in accordance with the principles specified in Section 6.1.3; and
- interaction between identically cloned systems which are controlled, designed and maintained by a single party – in accordance with the principle specified in Section 6.1.4

These circumstances will be reviewed from time to time to tie in with the trend of IT development in the Government. When in doubt, the IFCG should be consulted for clarification.

Although deviation from IF recommendations in these circumstances need not be reported as exemptions, such deviations must be documented in post-implementation departmental returns.

6. PRINCIPLES UNDERLYING THE RECOMMENDATION OF TECHNICAL STANDARDS

6.1 PRINCIPLES TO BE OBSERVED BY PROJECT TEAMS WITH REGARD TO THE USE OF THE IF TECHNICAL STANDARDS

6.1.1 General

- a. If an interoperability area that fits a project's usage requirement is found in the IF, project teams should base their new implementations on IF recommendations, including remarks on how to select among multiple standards. For interoperability areas and scope of usage not covered in the IF, project teams should negotiate with their interaction counterparts and agree on the interface; in doing so, project teams should observe the principle that open standards should be adopted where applicable.

6.1.2 Supporting multiple standards

- b. Different implementation choices and standards (including different versions of a standard) may be recommended under an interoperability area. Project teams should select the standard(s) that best fit their project requirements. Project teams should also decide whether to support different implementation choices and technical standards. In making this decision, project teams should assess the role and need of individual implementation, taking into consideration:
 - the computing environment of the interaction counterparts; and
 - whether it is cost-justified to support multiple implementation choices and standards.
- c. To maximize interoperability, a rule of thumb is that if an interface is targeted for **unknown counterparts** (i.e. in an **open** environment), the implementation should try to support as many **effective** implementation choices and recommended standards as possible, unless the cost precludes the need to do so.
- d. To better align with technology and market trends, when a new standard co-exist with an older version under IF recommendations, new implementations should try to support the new version as far as possible. And where backward compatibility solution exists, such solution should be implemented and tested, where necessary and applicable.

6.1.3 Managing existing systems

- e. As project teams manage **major** changes to existing systems, they should take into account technology and market trends and assess how to implement the changes cost-effectively. Since the IF is kept in line with technology and market trends, it will serve as a good reference for project teams.

-
- f. New connections to existing systems should take a pragmatic approach in respect of IF conformance; conformance to the IF should be considered when a cost/benefit analysis indicates merits in adopting IF standards.

6.1.4 Interaction between identically cloned systems that are controlled, designed and maintained by a single party

- g. When a single party designs a common application for running in different B/Ds and the identically cloned systems running in different B/Ds interact with each other, even though that single party has total control over the implementation and maintenance of those systems, it should also design the system interface to conform to the IF as far as practical, because this will allow more flexibility for further development. However, there may be cases where a more proprietary interface mechanism between the identically cloned systems is more efficient, e.g. to save data transformation at both ends of the interface. Using such a proprietary interface mechanism should not be construed as a violation of the IF principles as long as the “proprietary interface” is not a reason to dictate B/Ds to use the identically cloned systems. Having said that, any interface from those cloned systems to any external system must be IF compliant.

6.2 PRINCIPLES FOR INCLUDING INTEROPERABILITY AREAS UNDER THE IF

- a. The IFCG will co-ordinate the recommendation of technical standards that generically apply across B/Ds. For industry specific interoperability areas that affect multiple B/Ds, the IF will provide a link to domain specific standards defined by other B/Ds that possess the domain knowledge;
- b. Areas should be included only when there is a business need to do so (see Note 1);
- c. Areas should be included when there is an over-riding technical need to do so, for example domain name service and LAN/WAN Interworking;
- d. Areas where the choice of standards primarily depends on an external service provider providing related services to the Government should not be included. For example, in mobile computing, we expect the mobile network operator will decide which 3G standards to adopt in providing mobile services that are interoperable with the rest of the industry;
- e. An area should be included only when it directly impacts interoperability, i.e. where a common specification is required to enable two parties to communicate;

-
- f. The majority of areas will focus on the interactions between computer systems e.g.
 - Information interchange between two or more discrete application systems, both direct and through removable storage media
 - Interaction between some central infrastructure services (e.g. a shared transaction portal similar to the Electronic Service Delivery (ESD) front end) and the systems that use those infrastructure services (e.g. the departmental systems in various B/Ds that support the ESD-like transactions in the backend)
 - The format for exchanging documents between the computer systems used by different users
 - Security specifications to enable secure communication between two parties as required.
 - g. Some areas will focus on the open standards for one party to control certain behaviour of another party's computer system; e.g. the various markup languages such as HTML, WML, that allow the content author to control the display of content on another party's computer;
 - h. Areas are not required if they are implied by other interoperability areas. For example, an interoperability area is not required for Control Protocol for LAN/WAN Interworking (where specifications such as ICMP would be specified) as it is implied by the LAN/WAN Interworking interoperability area.

Note 1: Areas where there is a business need but where standards are immature will be included as areas for future consideration.

Note 2: Areas where it is envisaged it will satisfy a future business need, even if that need is currently not present, will also be included as areas for future consideration.

Note 3: With regard to the naming of the areas, we adopt the following principles:

- Areas should accurately reflect the scope of usage of the technical standards;
- Areas should be defined in such a way as to not restrict implementation choices, for example 'Mobile device Internet access' rather than 'WAP';
- Areas should, wherever possible, be consistent with those defined in related Government standards and frameworks;
- Areas should be flexible to ensure that they can accommodate future developments.

6.3 PRINCIPLES FOR SELECTING TECHNICAL STANDARDS UNDER THE IF

- a. The specifications adopted should be either internationally recognised or *de facto* standards that are mature and are widely used in the industry
- b. Mature and widely adopted open standards should be considered in favour of their proprietary alternatives
- c. The specifications adopted should be vendor and product neutral as far as possible;

-
- d. For any particular purpose, the number of specifications allowed should be limited as far as practicable in order to minimise the cost and complexity for the Government to support those specifications, provided that such limited choice will not cause too much inconvenience to members of the public;
 - e. Without violating the principle of minimising the set of allowed specifications, the number of specifications chosen for each area should provide an appropriate level of flexibility without compromising the overall objective of interoperability;
 - f. The specifications should be well aligned with Internet (e.g. W3C and IETF) standards as the Internet is a major channel for delivering e-Government services;
 - g. Specifications will be selected which support the requirements of electronic submissions under law together with any additional requirements specific to the interactions between B/Ds and their business partners within or external to the Government;
 - h. The industry should be involved when determining the specifications or schemas to be adopted for a vertical sector;
 - i. Local, regional and international developments should be taken into consideration and, in particular, the development of standards in the wider Chinese community. The specifications adopted should take account of similar foreign government initiatives elsewhere demonstrating best practice;
 - j. Where appropriate, specifications should be adopted which are consistent with current HKSARG standards specifications and frameworks;
 - k. If a specification is implied by a higher level specification (e.g. the encryption algorithms RC4 and DES used by the transport level security standard SSL), then there is no need to specify it unless it is also applicable to another interoperability area (e.g. DES is also included as a symmetric encryption algorithm used independently of SSL);
 - l. Consideration should also be given to the likely evolution of the mature specification, in the light of emerging standards and technologies, to minimise the likelihood of obsolescence of the mature standard;
 - m. Versions of standards will need to be updated as new functionality is introduced and new versions become widely adopted by industry. Special attention will be paid to backward compatibility to minimise the impact of the transition to a new version of a specification, thereby facilitating continued interoperability;
 - n. Prevailing IF standards that, regardless of versions, are no longer widely used in the open environment should be removed from the IF;
 - o. When there is a new replacement to serve the same function, an old standard should be removed from the IF, unless :

- the old standard is still widely used in an open environment; or
- there is concern requesting existing users of the old standard to adopt a new standard (e.g. additional resources will be required from them) and compatibility between the old and new standards can be managed

Version numbers of technical specifications are selected to provide the appropriate level of functionality to meet the business and technical requirements. However, there are several cases where version number issues arise. The following principles clarify the rationale for selecting specific versions of specifications:

- p. Where applicable, the specification should be unambiguous so that the user of the specification knows exactly which standard or version of a standard to follow (in order for him to verify whether his work complies to the specification or not); this could be done through various means, e.g. by stating a reference document where the standard is published, or by referring to a reference implementation, e.g. Netscape Mail 7.0, etc.;
- q. In some cases, the functions of a particular standard (e.g. HTML and S/MIME) may not be fully implemented in some products, or a product may have implemented its own extensions. And in some cases, a product may not mention which version of a standard it is supporting. In such cases, it may be more practical to specify which are the products and versions that the receiving party is likely to use, so that the sender can generate messages / files that will be compatible with the application used by the receiving party;
- r. For specifications not related to submissions under law, if the software the receiving party needs to process the information / document is free, in most cases the version of the specification need not be mandated; however, the sender has the obligation to inform the receiving party which software (and versions of the software) is best for processing the information / document;
- s. For specifications related to submissions under law, there is a need to limit the number of allowed versions of a specification so that B/Ds can use a stable platform to process the submissions;
- t. Version numbers are selected to provide a broad range of product and/or technical compliance. They are also selected to cover the broadest practical extent of adoption – standards should be in common usage and/or readily implementable. The selected version may not be the latest available version: this is because the selected version meets the functional requirements and remains in popular usage;
- u. In selecting versions of standards, the implications on the user community are always considered. Specifying a recent version of a standard may require the Government, its agencies, and/or the public (citizens and businesses) to upgrade their technical environments and may cause expense to be incurred;

Note 1: Internationally recognised (e.g. ISO, IETF, W3C) or *de facto* standards relevant to an interoperability area would be included as candidate standards⁵ for consideration.

Note 2: While only mature standards will be adopted, prominent emerging standards should be closely monitored for potential future adoption.

Note 3: Normally, new versions of the recommended standards will not be listed as an emerging standard although the new versions are likely to replace the currently recommended version in the future, except where there is a major difference between the current version and the new version. For example, when WAP v1.2 was the recommended standard, WAP 2.0 was not listed as an emerging standard. In contrast, since there is a significant difference between IPv4 and IPv6, IPv6 is listed as an emerging standard along with IPv4 as a recommended standard.

Note 4: When multiple implementation choices or standards are recommended for an interoperability area, remarks should be provided on how the interacting parties may choose among the multiple standards, where necessary.

Note 5: When multiple standards are recommended for an interoperability area, the IF should recommend best practices for addressing interoperability among the different standards as necessary.

⁵ The candidate standards are listed in the “Analysis Underpinning the HKSARG Interoperability Framework Recommendations”, which is a document in the IF document library.

7. SPECIFICATIONS UNDER THE INTEROPERABILITY FRAMEWORK

7.1 OVERVIEW

The specifications under the HKSARG Interoperability Framework currently include:

- Specifications in Sections 7.2 to 7.5 of this document;
- Common Schemas published on the registry at www.xml.gov.hk;
- Computer-Aided-Drafting Standard for Works Projects;
- Final Report on Implementation of Data Alignment Measures for the Alignment of Planning, Lands and Public Works Data;
- Guidelines on Dissemination of Information through Government Homepages;
- LAN Addressing and Naming Standard; and
- XML Schema Design and Management Guide.

All specifications under the IF are accessible from the IF homepage.

Sections 7.2 to 7.5 below cover the technical standards which are grouped into a number of high-level categories referred to as Interoperability Domains:

- 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.

Under each of these domains, there are a number of Interoperability Areas that define with more granularity where technical specifications to facilitate interoperability need to be identified.

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 specifications are recommended based on analysis documented in the "Analysis Underpinning the HKSARG IF Recommendations" which is posted on the IF homepage.

7.2 APPLICATION INTEGRATION DOMAIN

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
Simple functional integration in an open environment (e.g. information retrieval from a remote application)	The suite of core Web Services standards : SOAP v1.1 for remote service invocation WSDL v1.1 for remote service description (where necessary) UDDI v2 for the publication and discovery of remote service descriptions	No	When project teams select products to implement Web Services, they are recommended to take into consideration the products' conformance to the WS-I's Basic Profile 1.0. In addition, project teams should implement their Web Services requests and responses in accordance with the WS-I Basic Profile 1.0.
Reliable document exchange between application systems in an open environment for business document-oriented collaboration	ebMS v2	B/Ds will promulgate explicit requirements where relevant	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 document exchange. Although ebMS is not widely supported by the major vendors, its open source implementations can be considered
Secure exchange of messages in a Web Services environment	WS-Security 1.0	No	Project teams should closely monitor the development of the WS-I Basic Security Profile and follow its recommendations when it is ratified.

7.3 INFORMATION ACCESS AND INTERCHANGE DOMAIN

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
Hypertext Web content	HTML and XHTML as implemented by commonly adopted versions of browsers	No	The content providers should state on their Web page how the content can best be viewed. They are also recommended to test their content against different combinations of popular browser and operating system configurations.
Client-side scripting	ECMA 262 Script 3 rd Edition	No	

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
Mobile Web content	<p>WML 1.3 – for use with WAP devices</p> <p>HTML and XHTML as implemented by commonly adopted browsers on mobile devices – for use with mini-browsers</p> <p>XHTML Mobile Profile v1.1 – for use with mini-browsers on resource-constrained devices like mobile phones</p>	No	Content authors are recommended to test their content against different popular browsers.
Document file type for content publishing	<p>HTML and XHTML as implemented by commonly adopted versions of browsers</p> <p>PDF</p>	No	<p>The HTML content providers should state on their document how the content can best be viewed. They are also recommended to test their content against different combinations of popular browser and operating system configurations</p> <p>The PDF content providers should indicate which viewer software the recipients can use and supply a link to the viewer software if necessary.</p>
Document file type for receiving documents under ETO	<p>.txt</p> <p>.rtf v1.6</p> <p>HTML</p> <p>PDF v1.2, 1.3, 1.4, 1.5 or 1.6</p>	see Note 1	For HTML file types, members of the public should use only those HTML features that are implemented in common by Microsoft Internet Explorer v6.x and Netscape v8.x / Firefox v1.x.
Attachment of digital signature to electronic documents received under ETO	<p>PKCS #7 v1.5 (RFC 2315)</p> <p>S/MIME v3</p> <p>PDF v1.5 or 1.6</p>	see Note 1	For electronic submissions via email pursuant to the ETO, members of the public should use only those S/MIME v3 features that are implemented in common by Microsoft Outlook Express 6.x and Netscape Mail 7.x.
Formatted document file type for collaborative editing	<p>.rtf v1.6</p> <p>HTML and XHTML as implemented by commonly adopted versions of browsers</p> <p>.doc (Word 97 file format which is used by Word 97 and later versions)</p> <p>.sxw</p> <p>OpenDocument 1.0</p>	No	<p>If the sender is uncertain what office software the recipients are using, the sender should send the documents in a format (e.g. .htm, .rtf, .doc) that common office software available in the market are able to handle. However, if both sides are using office software that belong to the same family, then tool-specific format like .sxw may be used for file exchange.</p> <p>B/Ds should refer to ITSD Circular No. 8/2003 (Exchanging Electronic Documents Involving Different Office Software Products) for guidelines on how to reduce their exposure to incompatibility problems arising from the mixed use of</p>

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
			different office software products or different versions of the same product in a user community.
Presentation file type for collaborative editing	.ppt (PowerPoint 97 file format which is used by PowerPoint 97 and later versions) .sxi OpenDocument 1.0	No	<p>If the sender is uncertain what office software the recipients are using, the sender should send the presentation in a format (e.g. .ppt) that common office software available in the market are able to handle. However, if both sides are using office software that belong to the same family, then tool-specific format like .sxi may be used for file exchange.</p> <p>B/Ds should refer to ITSD Circular No. 8/2003 (Exchanging Electronic Documents Involving Different Office Software Products) for guidelines on how to reduce their exposure to incompatibility problems arising from the mixed use of different office software products or different versions of the same product in a user community.</p>
Spreadsheet file type for collaborative editing	.xls (Excel 97 file format which is used by Excel 97 and later versions) .sxc OpenDocument 1.0	No	<p>If the sender is uncertain what office software the recipients are using, the sender should send the spreadsheet in a format (e.g. .xls) that common office software available in the market are able to handle. However, if both sides are using office software that belong to the same family, then tool-specific format like .sxc may be used for file exchange.</p> <p>B/Ds should refer to ITSD Circular No. 8/2003 (Exchanging Electronic Documents Involving Different Office Software Products) for guidelines on how to reduce their exposure to incompatibility problems arising from the mixed use of different office software products or different versions of the same product in a user community.</p>
E-mail format	MIME (RFCs 2045, 2046, 2047, 2048, 2049, 2231, 2387, 2392, 2557, 2646, 3023)	Yes	
E-mail security	S/MIME v3	Yes	For electronic submissions via email pursuant to the ETO, members of the public should use only those S/MIME v3 features that are implemented in common by Microsoft Outlook Express 6.x and Netscape Mail 7.x.

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
Graphical / Image file types	<p>.jpg – for images that will tolerate information loss</p> <p>.gif v89a – for images that will tolerate information loss with few colours and limited graduation between colours</p> <p>.tif v6 – good for images that will not tolerate information loss</p> <p>.png second edition – as an alternative to gif v89a offering greater compression and where control over transparency is required</p> <p>epsf v3 – for images that require editing and/or which are included in PostScript printed output</p>	Yes	
Character sets and encoding for Web content	<p>ISO/IEC 8859-1:1998 – for encoding content in English</p> <p>BIG-5 and HKSCS-2001 – for encoding content in Chinese</p> <p>ISO/IEC 10646-1:2000 and HKSCS-2001 – for encoding content in English or Chinese (Chinese characters are restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO 10646 standard and the HKSCS-2001).</p>	No	<p>For the correct display of Web content, the content provider should specify the character encoding in the document explicitly.</p> <p>ISO 10646 is the standard for the common Chinese language interface, B/Ds are recommended to adopt ISO 10646, where applicable.</p> <p>The development of the IICORE, which is a subset of the ISO 10646 standard (comprising the most commonly used characters) designed for use on resource-limited devices, will be closely monitored and reflected in the future releases of the IF. Content providers that are developing content for resource-limited devices (such as mobile phones) are advised to take note of the developments of IICORE.</p>

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
Character sets and encoding for other types of information exchange	ASCII – for encoding content in English BIG-5 and HKSCS-2001 – for encoding content in Chinese ISO/IEC 10646-1:2000 and HKSCS-2001 – for encoding content in English or Chinese (Chinese characters are restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO 10646 standard and the HKSCS-2001).	Yes	Where applicable (e.g. in XML documents), the content provider should specify the character encoding in the document explicitly (e.g. use <code><?xml encoding='UTF-8'></code> to specify the UTF-8 encoding in an XML document). ISO 10646 is the standard for the common Chinese language interface, B/Ds are recommended to adopt ISO 10646, where applicable. The development of the IICORE, which is a subset of the ISO 10646 standard (comprising the most commonly used characters) designed for use on resource-limited devices, will be closely monitored and reflected in the future releases of the IF. Content providers that are developing content for resource-limited devices (such as mobile phones) are advised to take note of the developments of IICORE.
Compressed files	.zip .gz v4.3	Yes	
Removable storage media for receiving documents under the ETO	3.5” 1.44MB floppy diskette in MS-DOS format CD-ROM in ISO 9660:1988 format	Yes	
Animation	Macromedia Flash (.swf) Apple Quicktime (.qt, .mov, .avi) Macromedia Shockwave (.swf)	No	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.
Moving image and audio / visual	MPEG-1 (ISO 11172) – for video and audio .mp3 (ISO 11172) – for audio	No	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.
Audio / video streaming	Real Audio / RealVideo (.ra, .ram, .rm, .rmm) Windows Media Formats (.asf, .wma, .wmv)	No	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.

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
E-Business document / data message formatting language	XML and related W3C recommendations produced by the W3C XML Core Working Group	Business specific XML schemas will be published where relevant	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.
XML schema definition	XML Schema 1.0 – for data-oriented message DTD as defined in the corresponding XML specification – for textual document-oriented applications	Business specific XML schemas will be published where relevant	
XML message encryption	XML Encryption	To be specified along with the business specific XML schema	
XML message signing	XML Signature	To be specified along with the business specific XML schema	
Content syndication	RSS 1.0 or RSS 2.0	No	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.

Note 1: There is some difference between the recommended specification and the format stated in the Format and Manner Requirements that prevail when this version of the IF is published. The recommended specification is intended to be relevant for electronic submission under the ETO and when this version of the IF becomes effective, this and any other relevant specifications will be promulgated to the public through a government notice published in relation to the Format and Manner Requirements.

7.4 SECURITY DOMAIN

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
IP network-level security	IPsec	No	
Transport-level security	SSL v3.0 TLS v1.0	No	New implementations should ready themselves to support TLS and should ensure their TLS implementation's backward compatibility with SSL v3 where situation allows
Symmetric encryption algorithms	DES 3DES – comparatively harder to break AES – comparatively harder to break	No	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 strength. The interacting parties should either agree before implementation on the algorithm to use or should enable some auto-negotiation mechanism.
Asymmetric encryption algorithms	RSA	No	
Digital signature algorithms	DSA RSA for Digital Signatures	No	The interacting parties should either agree before implementation on the algorithm to use or should enable some auto-negotiation mechanism.
Hashing algorithms for digital signature	SHA-1	No	
Cryptographic message syntax for file-based signing and encrypting	PKCS #7 v1.5 (RFC 2315)	No	
On-line certificate status protocol	RFC 2560	No	
Certification request	PKCS #10 v1.7 (RFC 2986)	No	
Certificate profile	RFC 3280 (X.509 v3)	No	
Certificate revocation list profile	RFC 3280 (X.509 v2)	No	
Certificate import / export interface	PKCS #12 v1.0	No	
Cryptographic token interface	PKCS #11 v2.11 Microsoft CryptoAPI	No	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.

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
Cryptographic token information syntax	PKCS #15 v1.1	No	
Privacy policy	P3P v1.0	No	
Exchange of authentication and authorisation information	SAML v1.1	No	
Time stamping protocol	RFC 3161 (X.509 PKI TSP)	No	

7.5 INTERCONNECTION DOMAIN

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
E-mail transport	SMTP (RFCs 2821, 2822)	Yes	
Mail box access	POP3 – for basic mail box access IMAP4 rev1 – for more advanced functionality allowing clients to manipulate messages on the server	No	
Hypertext transfer protocol	HTTP/1.1	No	
Directory access	LDAP v3	No	
Domain name service	DNS	No	
File transfer	FTP HTTP/1.1 SFTP	No	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 SSL/TLS to avoid having to install client-side software.
LAN / WAN interworking	IPv4	No	
LAN / WAN	TCP – preferred transport	No	

Interoperability area	Recommended specification(s)	Are the specifications relevant to submissions under ETO ?	Remarks
transport protocol	protocol over UDP UDP – where required e.g. to support particular protocols		
Wireless LAN	IEEE 802.11b IEEE 802.11g	No	Products of Wireless LAN with Wi-Fi Certification are recommended in order to ensure the interoperability between different manufacturers. All new access points are highly recommended to support IEEE 802.11g. New client devices are also recommended to support IEEE 802.11g where possible.
Wireless LAN security	WPA	No	
Mobile device Internet access	WAP v2.0 – for use with WAP devices HTTP/1.1 – for use with mini-browser	No	

7.6 OTHER SPECIFICATIONS UNDER OBSERVATION

The technical specifications listed below are under observation either because the need to address the interoperability area is not imminent or the specifications are not matured / widely adopted yet. Please refer to the document "Analysis Underpinning the HKSARG IF Recommendations" for details.

Domain	Interoperability area	Specification(s) under observation
Application integration	Simple functional integration in an open environment	WSIL for locating WSDLs directly from the service provider's site.
	Reliable document exchange between application systems in an open environment for business document-oriented collaboration	WS-Reliability WS-ReliableMessaging
	Intra-government workflow and business process management	BPML WS-BPEL Web Services Choreography BPSS
	Information model for e-business registry	ebXML Registry Information Model
	E-business registry service	ebXML Registry Service Specification
Information access and	Attachment of digital signature to electronic documents received under ETO	Cryptographic Message Syntax (CMS) (RFC 3369)

Domain	Interoperability area	Specification(s) under observation
interchange	Formatted document file type for collaborative editing	WordProcessingML
	Spreadsheet file type for collaborative editing	SpreadsheetML
	Compressed files	.rar
	Removable storage for receiving documents under the ETO	DVD-ROM in ISO/IEC 13346:1995 format
	Moving image and audio/visual	MPEG-4 (ISO 14496)
	Audio/video streaming	MPEG-4 (ISO 14496)
	XML schema definition	Relax NG
	Content syndication	Atom
	Vector graphics (non GIS/mapping application)	Scalable Vector Graphics
	Content/data resource description language	Resource Description Framework
	Inter-organisation radio frequency identification	The suite of RFID related specifications from EPCglobal
	Electronic form (see Remark at end of table)	XForms
Security	Asymmetric encryption algorithms	Elliptic Curve Cryptography (ECC) (RFC 3278)
	Digital signature algorithms	ECDSA
	Hashing algorithms for digital signature	SHA-224, SHA-256, SHA-384, SHA-512
	Cryptographic message syntax for file-based signing and encrypting	Cryptographic Message Syntax (CMS) (RFC 3369)
	Certification request	Certificate Request Message Format (CRMF) (RFC 2511)
	XML-based authorisation and entitlement	XACML
	XML key management	XKMS
Interconnection	Domain name service	IDN
	LAN/WAN interworking	IPv6
	Wireless LAN	IEEE 802.11a
	Wireless LAN security	WPA2 and IEEE 802.11i

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

8. GOVERNMENT NETWORK ARCHITECTURE

8.1 OVERVIEW

The Government Network Architecture (GNA) defines the organisation of and the relationships between components of the Government's IT infrastructure. These components include Departmental Networks (DNs), Common Services (CSs), External Access Gateways (EAGs) and the Government Backbone Network (GNET).

For details of a particular DN, please contact the respective IT Management Unit or the Departmental Liaison Officer. For details of a particular CS, please contact the respective service provider.

Connections to GNET from non-Government networks or external parties must be via external access gateway whose GNET connection is based on the GNET supported network protocols.

8.2 MAJOR COMPONENTS OF THE GNA

The GNA defines the relationships between the major building blocks of the Government-wide IT infrastructure. These major components are:

A. Departmental Networks (DNs)

DNs are networks established by B/Ds themselves to facilitate the data communication requirement within respective B/Ds. A DN is connected to the GNET to enable communication with other B/Ds and to provide access to the CSs. Typically, for resilience, each DN has two connection points with the GNET. DN users can access a number of available Common Services via these connection points. B/Ds can also make use of the GNET to establish communication channels with other departments.

B. Government-wide Common Services (CSs)

Common Services are infrastructure components that provide shared Government-wide services, for use by B/Ds. All B/Ds can access Common Services via the GNET rather than through direct connections to each CS. Examples of CSs are the Central Cyber Government Office (CCGO), the Central Internet Gateway (CIG), the Government Communication Network (GCN), and Government Directory Services (GDS).

C. Government Backbone Network (GNET)

The GNET is the core data transport network of the GNA that facilitates interconnection between the various DN and CSs. Currently, it consists of a number of routers and switches located in the OGCIO Central Computer Centres and various Government buildings.

D. External Access Gateway (EAG)

EAG is a connection point to GNET from non-government or external networks. The main function of EAG is to protect the government networks and to stop any unauthorized and malicious traffic from the external parties entering GNET. For projects, CSs or DNs that would like to acquire services from external parties through GNET, they should setup and manage the EAG for connecting GNET at one end and the external parties at the other.

8.3 COMPLIANCE AND ADOPTION OF THE GNA

In accordance with the GNA, each B/D is required to deploy its own departmental network (DN) and connect to the GNET in order to access Common Services and to connect to other departments. This allows the Government to maximise the cost effectiveness and minimise the complexity of the overall Government network.

New projects that require inter-departmental communication and access to Common Services are required to conform to the GNA. Existing legacy workgroup networks and project-specific networks, if any, are required to conform to the GNA when there is a need to integrate with other components through the GNET.

8.4 NETWORK ARCHITECTURE

The network architecture aims:

- To provide a core data transport network to connect B/Ds to CSs; and
- To provide a channel for inter-departmental communication.

The diagram below illustrates the organisation of the GNA and the relationship between its four core components.

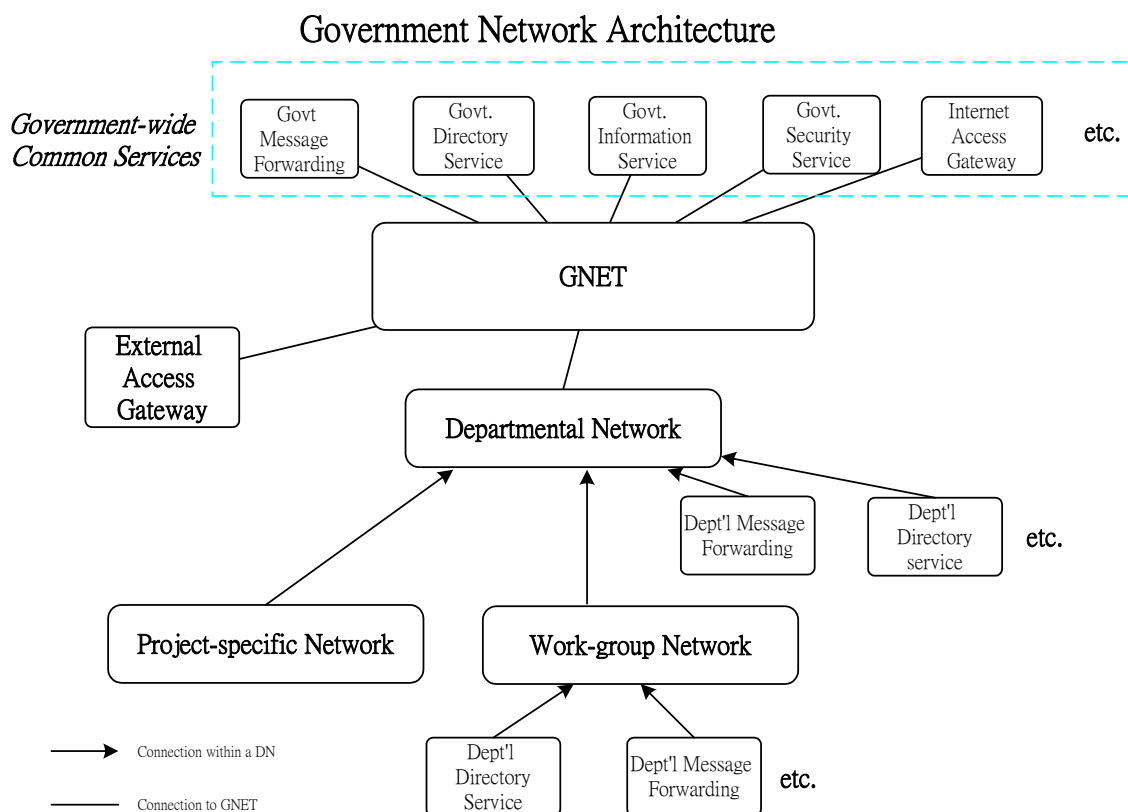


Diagram 8.1 – The Government Network Architecture

8.5 NETWORKING PROTOCOLS CURRENTLY SUPPORTED BY THE GNET

The core data transport network in the GNET is based on a number of proven, mature and widely adopted network protocols:

- IP – the network layer protocol;
- BGP-4 – the IP-routing protocol for routers in DN's and the GNET.

Each DN/CS/EAG is defined as an Autonomous System (AS) and is given a unique AS number in accordance with the LAN Addressing and Naming Standard. The GNA does not define the Interior Gateway Protocol (IGP) to be deployed within the DN or CS, although OSPF is generally recommended.

Edge routers used for interconnection between DN's, EAG's, the GNET and the CS's utilise IP and BGP-4.

In order to meet a variety of Government connection requirements, the GNET supports a number of physical and data-link network standards, in line with network industry trends and GNET capabilities:

- Point-to-Point Protocol (PPP);
- IEEE 802.3 (commonly referred as Ethernet);
- Frame Relay;
- Asynchronous Transfer Mode Adaptation Layer Type 5 (AAL5).

The following table summarises the protocols which are currently supported by the GNET for interconnection between DNs and CSs. These protocols will be reviewed by the GNET service team periodically. B/Ds should refer to the ITG InfoStation for the latest GNET service offering.

Type of Protocol	Name of Protocol
Network layer protocol	IP
Routing Information Protocol	BGP-4
Data Link Protocol	PPP, IEEE 802.3, Frame Relay and AAL5

Table 8.1 – Summary of networking protocols currently supported by the GNET

9. ABBREVIATIONS AND ACRONYMS

3DES	Triple Data Encryption Standard
3G	Third Generation mobile phones
AAL5	Asynchronous Transfer Mode Adaptation Layer Type 5
AES	Advanced Encryption Standard
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
B/D	Bureau/Department
BGP	Border Gateway Protocol
BIG-5	The Standard for the Coding of Chinese Characters Promulgated by the Institute for Information Industry of Taiwan
BPML	Business Process Management Language
BPSS	Business Process Specification Schema
CAD	Computer-Aided-Drafting
CIG	Central Internet Gateway
CRMF	Certificate Request Message Format
CS	Common Service
DES	Data Encryption Standard
DN	Departmental Network
DNS	Domain name services
DSA	Digital Signature Algorithm
DTD	Document Type Definition
EAG	External Access Gateway
EBCDIC	Extended Binary-Coded Decimal Interchange Code
ebMS	ebXML Message Service
ebXML	Electronic Business eXtensible Markup Language
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMA	European Computer Manufactures Association
EPC	Electronic Product Code
EPSF	Encapsulated PostScript File
ESD	Electronic Service Delivery
ETO	Electronic Transactions Ordinance
FTP	File Transfer Protocol
GCN	Government Communication Network
GDS	Government Directory Services
GNA	Government Network Architecture
GNET	Government Backbone Network
HKSARG	The Government of the Hong Kong Special Administrative Region
HKSCS	Hong Kong Supplementary Character Set
HTML	HypertText Markup Language
HTTP	Hypertext transfer protocols
ICMP	Internet Control Message Protocol
IDN	Internationalized Domain Name
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IF	Interoperability Framework
IFCG	Interoperability Framework Co-ordination Group
IGP	Interior Gateway Protocol
IICORE	International Ideographs Core
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
ITG InfoStation	IT in Government Information Station
ITMU	IT Management Unit
ITSD	Information Technology Services Department (replaced by Office of the Government Chief Information Officer)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDUP	LDAP Duplication / Replication / Update Protocol
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MS-DOS	Microsoft Disk Operating System
OGCIO	Office of the Government Chief Information Officer
OSPF	Open Shortest Path First
P3P	Platform for Privacy Preferences Project
PDF	Portable Document Format
PKCS	Public Key Cryptography Standards
PML	Physical Markup Language
POP	Post Office Protocol
PSC	Project Steering Committee
RC4	Rivest's Cipher 4
RFC	Request for Comments
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
S/MIME	Secure Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language
SFTP	SSH File Transfer Protocol
SHA-1	Secure Hash Algorithm 1
SMTP	Simple Message Transfer Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDDI	Universal Description Discovery and Integration
UDP	User Datagram Protocol
UN/EDIFACT	United Nation / Electronic Data Interchange for Administration, Commerce and Transport
UTF	Universal Transformation Format
W3C	World Wide Web Consortium
WAE	Wireless Application Environment
WAN	Wide Area Network
WAP	Wireless Application Protocol
WML	Wireless Markup Language

WPA	Wi-Fi Protected Access
WSDL	Web Services Description Language
WS-BPEL	Web Services Business Process Execution Language
WS-I	Web Services Interoperability Organisation
WSIL	Web Services Inspection Language
XACML	eXtensible Access Control Markup Language
XHTML	Extensible HyperText Markup Language
XKMS	XML Key Management Specification
XML	Extensible Markup Language
XMLCG	XML Co-ordination Group