
# The HKSARG Interoperability Framework

Version : DRAFT FOR CONSULTATION

**Jul 2002**

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

Interoperability Framework

Prepared By: Coordination Group Copy No: _____

Doc. Effective Date: _____ Doc. Expiry Date: _____

Endorsed By: _____ Authorized By: _____

Date: _____ Date: _____

| Amendment History | | | | |
|---|---|---|---|---|
| Change Number | Revision Description | Pages Affected | Revision Number | Date |
| | | | | |

# 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 XML SCHEMAS ..... 4-2
4.4 CHANGE MANAGEMENT ..... 4-3

**5. COMPLIANCE ..... 5-1**

5.1 THE USE OF TECHNICAL SPECIFICATIONS AND PUBLISHED CORE XML 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 ..... 5-2
5.5 RESPONSIBILITIES ..... 5-3
5.6 PROCEDURES FOR EXEMPTION FROM COMPLIANCE ..... 5-3

**6. PRINCIPLES FOR INCLUDING INTEROPERABILITY AREAS AND SELECTING TECHNICAL SPECIFICATIONS ..... 6-1**

6.1 SPECIFYING THE INTEROPERABILITY AREAS ..... 6-1
6.2 SELECTING THE TECHNICAL SPECIFICATIONS ..... 6-2

**7. RECOMMENDED SPECIFICATIONS FOR THE INTEROPERABILITY AREAS 7-1**

7.1 INTEROPERABILITY DOMAINS ..... 7-1
7.2 DOMAIN 1: BUSINESS SPECIFIC ..... 7-1
7.3 DOMAIN 2: APPLICATION INTEGRATION ..... 7-1
7.4 DOMAIN 3: INFORMATION ACCESS AND INTERCHANGE ..... 7-2
7.5 DOMAIN 4: SECURITY ..... 7-4
7.6 DOMAIN 5: INTERCONNECTION ..... 7-6

**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

# 1. EXECUTIVE SUMMARY

The Interoperability Framework 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 Interoperability Framework defines a collection of specifications aimed at facilitating the interoperability of Government systems and services, plus the adoption of eXtensible Markup Language (XML) for enabling the sharing of data and information between these systems.

With the emergence of Government systems making use of XML, XML schemas will be adopted / developed to meet specific business application needs. These XML schemas will form part of the Interoperability Framework.

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.

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 should be developed based on the Interoperability Framework. E-Government applications that depend on, or communicate with those infrastructure systems should therefore comply with the Interoperability Framework to facilitate better integration.

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

For existing systems, given the diversity of current platforms and systems, conformance to certain specifications may not be readily achieved. Existing systems should conform to the Interoperability Framework 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 Interoperability Framework should be considered when a major functional change is being performed, and it is financially and functionally prudent to introduce compliance with the Interoperability Framework.

The development of an Interoperability Framework 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 Interoperability Framework will be reviewed every 6 to 12 months.

# 2. PURPOSE AND STRUCTURE OF DOCUMENT

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

The information is arranged as follows:

- Section 3 provides an overview of the Interoperability Framework, including its objectives, and scope;
- Section 4 covers the management of the Interoperability Framework, including terms of reference for the governance bodies, membership criteria, and change management issues;
- Section 5 describes Interoperability Framework compliance, including compliance policy, responsibilities and procedures for exemption;
- Section 6 includes the principles for selecting the interoperability areas and the technical specifications;
- Section 7 lists the technical specifications selected for the identified interoperability areas;
- Section 8 describes the Government Network Architecture.

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

The Interoperability Framework Coordination Group (IFCG)
Information Technology Services Department

Email: ifcg@itsd.gov.hk

Note : The Government reserves the right to publish all views and comments submitted in respect of the Interoperability Framework and to disclose the identity of the source. Accordingly any part of the submission which is considered to be commercially confidential should be clearly marked and supported by reasons why such confidentiality is claimed. We will take such markings and claims into account in making decision as to whether to disclose such information or not.

# 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 Interoperability Framework is essential to support the flow of information and to improve the coherence of information systems maintained by individual B/Ds.

While current Government systems do interoperate satisfactorily, the integration of different systems often relies on proprietary solutions making it very costly and complicated to maintain. eXtensible Markup Language (XML) is widely recognised as a key technology in the development of cost-effective integration solutions.

The Interoperability Framework aims to define the set of specifications to enable Government systems to communicate and interoperate with other systems, both within Government and external to Government, efficiently and effectively. In addition, the Interoperability Framework promotes and fosters the adoption of XML to enable the exchange of data between applications.

The Interoperability Framework does not create technical standards. Rather, it defines the adoption of internationally recognised open and *de facto* standards.

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

## 3.2 SCOPE OF THE INTEROPERABILITY FRAMEWORK

The Interoperability Framework covers:

- A set of technical specifications defining the interface across different systems as well as the format for exchanging specific categories of information;
- Other specifications that define infrastructure architecture, conventions and procedures; and
- The adoption of XML for enabling the sharing of data and information between application systems.

Infrastructure architecture, conventions and procedures specifications supplement the technical specifications to facilitate interoperability. For example, the "ITSD LAN Addressing and Naming Standards" should be followed when B/Ds connect to common

services[1], 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), Central Services (CSs) and the Government Backbone Network (GNET). Please refer to section 8 for a description of the GNA.

Other conventions and procedures specifications in the Interoperability Framework document registry are published on the ' IT in Government Information Station' (ITG InfoStation) homepage on the Government-wide Intranet. B/Ds should refer to these when implementing e-Government services. Conventions and procedures specifications relevant to the public will also be published on the Internet.

The use of XML in sharing data and information between different Government systems implies that XML schemas will be adopted / developed to meet specific business application needs. These XML schemas will form part of the Interoperability Framework.

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. 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 Interoperability Framework will 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 Interoperability Framework. 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 Framework specifications might

[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.

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 Interoperability Framework 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 schemas 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 future data schemas used within Government, as well as to ensure prompt review and update of the set of specifications that comprise the Interoperability Framework. 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 data schemas or technical specifications, would be more effectively owned and managed by business application owners or dedicated specialist groups rather than under a common ownership; and
- Future changes to specifications, data schemas, etc. 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 Interoperability Framework, including the technical specifications, are managed by the **Interoperability Framework Co-ordination Group** and the XML schemas will be managed by the **XML Co-ordination Group** and the respective business application owners. The management mechanisms are described in the remainder of this section.

## 4.2 MANAGEMENT OF TECHNICAL SPECIFICATIONS

The overall Interoperability Framework, 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 Director of Information Technology Services 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 IT professionals from the Information Technology Services Department (ITSD) and other 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 ITSD.

Specialist groups in the ITSD, 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.

In addition, specialist groups in other B/Ds may take the lead in developing interoperability standards for their respective industries (e.g. Computer Aided Design standards for the construction industry). The IFCG will keep in close contact with these specialist groups and include relevant industry specific standards documents in the Interoperability Framework document registry.

## 4.3 MANAGEMENT OF XML SCHEMAS

Since the need for XML schemas stems from business requirements, business specific XML schemas should be developed by project teams formed by business users and system designers / developers representing the Government, plus other industry representatives as appropriate, for a particular business area.

Given the strategic nature of the initiative, and the need for a consistent approach, an XML Co-ordination Group (XMLCG) will be formed to develop 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 develop policies, guidelines and procedures to support the development and management of XML schemas for e-Government services;
- To oversee the development and management of XML schemas for e-Government services;
- To facilitate the sharing of experience in the use and implementation of XML.

The XMLCG reports to the Director of Information Technology Services and consists of professionals who are experienced in the adoption of XML in the public or private sector. In particular, B/Ds that participate in industry led XML initiatives will be invited to join the XMLCG.

The XMLCG will assess the feasibility of, and approach to developing resources for use by business specific project teams. Examples of such resources might include:

- Guidelines for designing XML schemas for e-Government services;
- Standard schemas for e-Government core data components (core schemas);
- A registry of XML schemas for e-Government services.

The publication of schemas in the registry and the use of those schemas will be governed by policies to be specified by the XMLCG. Subsequent maintenance of business specific XML schemas will be handled by the contributing application owners, plus additional stakeholders as appropriate.

## 4.4 CHANGE MANAGEMENT

The XML schemas, the Interoperability Framework document (i.e. this document), and associated specification documents will be published on the ITG InfoStation homepage on the Government-wide Intranet. The Interoperability Framework document and XML schemas relevant to the public will also be published on ITSD's homepage (www.itsd.gov.hk) on the Internet.

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

The development of an Interoperability Framework 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 specification documents. In order to facilitate the change cycle, the Interoperability Framework 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 ITSD Web site where relevant.

# 5. COMPLIANCE

## 5.1 THE USE OF TECHNICAL SPECIFICATIONS AND PUBLISHED CORE XML SCHEMAS

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

Compliance means B/Ds are expected to use those technical specifications and core XML schemas, plus the infrastructure architecture, conventions and procedures specifications listed in the Interoperability Framework document registry, where appropriate. For new systems where existing technical specifications or core schemas do not address interoperability requirements, a request for change should be raised.

## 5.2 COMPLIANCE POLICY

All new e-Government infrastructure systems, new government to public (including businesses) systems, and new inter-B/D systems should be developed based on the Interoperability Framework. E-Government applications that depend on or communicate with those infrastructure systems should therefore comply with the Interoperability Framework to facilitate better integration.

It is strongly recommended that all other new systems conform to the Interoperability Framework, 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 should conform to the Interoperability Framework 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 Interoperability Framework should be considered when a major functional change is being performed, and it is financially and functionally prudent to introduce compliance with the Interoperability Framework.

Outsourcing of Government systems implementation is a growing trend. The Interoperability Framework 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. In such cases, compliance with the Interoperability Framework should be specified as a requirement for the interface component(s).

In addition, business specific schemas will be developed with the participation of industry players, such that they address the needs of both Government and business. Any such business specific schemas developed should avoid conflict with the interoperability requirements of the Interoperability Framework as a whole. For example, business specific schemas should adopt the core schemas, where relevant, as far as possible.

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

There are, however, a number of specifications relevant to electronic submissions under the Electronic Transactions Ordinance (ETO). Once these specifications have been agreed after the consultation process, they will be reflected in the Format and Manner Requirements issued by the Secretary for Information Technology and Broadcasting pursuant to the ETO.

## 5.3 COMPLYING TO NEW VERSIONS OF THE INTEROPERABILITY FRAMEWORK

New systems or new integration projects should comply with the version of the Interoperability Framework effective on the date when budget was approved for the project. Should the Interoperability Framework be updated while the project is being implemented, such that the updated version impacts on that implementation, then a cost/benefit analysis should be undertaken to assess the feasibility of changing the system specification to align with the updated Framework.

## 5.4 WHO NEEDS TO UNDERSTAND COMPLIANCE

An understanding of the Interoperability Framework 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 Interoperability Framework (IF) at a high level and be aware that any systems involving interaction between B/Ds or between B/Ds and the public should comply with the IF;
- 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);
- 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 at a high level and ensure that IF compliance is taken into account during the project approval process;
- Government procurement officers - need to understand the IF at a high level to ensure that IF compliance is taken into account during the procurement of systems involved in inter-B/D or Government to public interactions;
- 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. The Head of a B/D's IT Management Unit (or its equivalent) has overall responsibility for ensuring compliance to the Interoperability Framework. Relevant stakeholders (e.g. project managers and application developers) should take individual responsibility for compliance.

Issues concerned with compliance with the Interoperability Framework 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 Interoperability Framework compliance.

## 5.6 PROCEDURES FOR EXEMPTION FROM COMPLIANCE

Should any IT project managers consider that there is a good case for exemption from compliance, the project manager may seek exemption approval from the Head of the concerned IT Management Unit (or its equivalent) with justifications made in writing.

Although compliance to the Interoperability Framework is governed on a self-regulatory basis, the Heads of IT Management Units of B/Ds (or their equivalent) are required to report to the IFCG within 2 weeks of approval for exemptions in relation to:

- new infrastructural systems (e.g. a shared transaction portal);
- new Government to public systems;
- new inter-B/D systems;
- new Government to public integration or inter-B/D integration initiatives based on existing systems.

Such reports will help the IFCG assess the applicability and effectiveness of the Interoperability Framework, with a view to developing a 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.

# 6. PRINCIPLES FOR INCLUDING INTEROPERABILITY AREAS AND SELECTING TECHNICAL SPECIFICATIONS

## 6.1 SPECIFYING THE INTEROPERABILITY AREAS

There are a number of guiding principles that determine which business and technical interoperability areas should be included under the Interoperability Framework. These are as follows:

a. Areas should be included only when there is a business need to do so (see Note 2);
b. Areas should be included when there is an over-riding technical need to do so, for example domain name service and LAN/WAN Interworking;
c. Areas where the choice of specifications 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;
d. 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;
e. The areas will focus on the interactions between computer systems e.g.
   - Data interchange between two or more discrete application systems
   - 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 secured communication between two parties as required.

Note 1: For industry specific areas, B/Ds are encouraged to include under the Interoperability Framework a link to the specifications they have agreed with the industry for specific purposes. This will facilitate the compilation of a central registry of all technical specifications and data schemas for the purpose of building interoperable e-Government systems.

Note 2: Areas where there is a business need but where standards are immature will be considered for inclusion in future versions of the Interoperability Framework and are not included in this document.

Note 3: Areas where it is envisaged it will satisfy a future business need, even if that need is currently not present, will also be considered for inclusion in future versions of the Interoperability Framework and are not included in this document.

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

f. Areas should be defined in such a way as to not restrict implementation choices, for example ' Mobile device Internet access' rather than ' WAP' ;

g. Areas should, wherever possible, be consistent with those defined in related Government standards and frameworks, for example the Technical Architecture for I-Net Government Applications (TAIGA);

h. Areas should be flexible to ensure that they can accommodate future developments.

## 6.2 SELECTING THE TECHNICAL SPECIFICATIONS

There are a number of guiding principles that determine how specifications should be selected for an interoperability area. These are as follows:

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 needs of inter-B/D interoperability within 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.

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:

k. The specification should be unambiguous so that the user of the specification knows exactly which specification or version of a specification 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 specification is published, or by referring to a reference implementation, etc.;

l. 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;

m. 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;

n. 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 – specifications 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;

o. In selecting versions of specifications, the implications on the user community are always considered. Specifying a recent version of a specification 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;

p. The Interoperability Framework is a flexible and updateable document, designed to reflect the current needs of the Government. Versions of specifications will need to be updated as new functionality is introduced and new versions become widely adopted by industry. The frequency of version updates is determined by the nature of each individual specification, which depends on functionality, ownership and adoption of that specification. Changes to the Interoperability Framework will be considered at regular intervals.

# 7. RECOMMENDED SPECIFICATIONS FOR THE INTEROPERABILITY AREAS

## 7.1 INTEROPERABILITY DOMAINS

The specifications are grouped into a number of high level categories, referred to as Interoperability Domains, which address different interoperability requirements:

- Business specific – message formats and semantics for data interchange between applications;
- Application integration – technical specifications to enable application-to-application integration;
- Information access and interchange – technical specifications for file exchange, character sets and encoding and content publishing;
- 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.

## 7.2 DOMAIN 1: BUSINESS SPECIFIC

In the business specific domain, we focus on message formats for data interchange between applications. For new implementations, XML should be adopted for data interchange across applications. The business specific XML schemas will be published in an XML registry for reference and use by B/Ds. XML schemas applicable to members of the public will be published on the Internet for reference by the public.

Other business message formats currently in use, e.g. UN/EDIFACT for exchanging EDI messages between Tradelink and the Government, will continue to be used until a commonly agreed alternate message format is available.

## 7.3 DOMAIN 2: APPLICATION INTEGRATION

| **Interoperability area** | **Recommended specification(s)** | **Specification(s) relevant to submissions under ETO** |
|---|---|---|
| Intra-government remote service delivery protocol (for integration of shared services and for simple application-to-application, functional integration) | • SOAP v1.1 | × |

| Interoperability area | Recommended specification(s) | Specification(s) relevant to submissions under ETO |
|---|---|---|
| Intra-government remote service description language | • WSDL v1.1 | × |
| Publication of intra-government remote services | • UDDI v1 | × |

## 7.4 DOMAIN 3: INFORMATION ACCESS AND INTERCHANGE

| Interoperability area | Recommended specification(s) | Specification(s) relevant to submissions under ETO |
|---|---|---|
| Hypertext Web content | • Htm(l) and xhtml implemented by commonly adopted versions of browsers | × |
| Client-side scripting | • ECMA 262 Script 3rd Edition | × |
| Web page design | • Web pages should be designed in accordance with the Guidelines on Dissemination of Information through Government Homepages | × |
| Speech | • VoiceXML 1.0 | × |
| Mobile device content | • WML v1.2 – for use with WAP devices<br>• HTML as implemented by commonly adopted browsers on mobile devices - for use with mini-browsers | ×<br>× |
| Content publishing | • Those parts of htm(l) commonly implemented by Netscape Navigator v4.7x and MS Internet Explorer v5.x<br>• PDF v3, 4 or 5 | ✓<br>✓ |
| Document file types | • .txt – for plain unformatted text<br>• .rtf v1.6 - for exchange between users using different word processing packages<br>• .doc (Word 97 file format) – for exchange between Microsoft Word users<br>• .sxw – for exchange between users of OpenOffice suite<br>• See Content publishing specifications | ✓<br>✓<br>×<br>×<br>✓ |

| Interoperability area | Recommended specification(s) | Specification(s) relevant to submissions under ETO |
|---|---|---|
| Presentation file types | • .ppt (PowerPoint 97 file format) – for exchange between Microsoft PowerPoint users<br>• .sxi – for exchange between users of OpenOffice suite<br>• see Content publishing specifications | ×<br>×<br>✓ |
| Spreadsheet file types | • .csv – for plain tabulated data<br>• .xls (Excel 97 file format) – for exchange between Microsoft Excel users<br>• .sxc – for exchange between users of OpenOffice suite<br>• See Content publishing specifications | ×<br>×<br>×<br>✓ |
| Graphical/still image file types | • .jpg – for images that will tolerate information loss<br>• .gif v89a - for images that will tolerate information loss with few colours and limited graduation between colours<br>• .tif v6 - good for images that will not tolerate information loss<br>(the choice of specification largely depends on the tool used to generate the image) | ✓<br>✓<br>✓ |
| Character sets and encoding | • ASCII – for encoding content in English<br>• BIG-5 – for encoding content in Chinese<br>• ISO 10646-1:2000 – for encoding content in English or Chinese (with Chinese characters restricted to the Chinese-Japanese-Korean Unified Ideographs characters coded in the ISO 10646 standard)<br>• HKSCS (issued in 1999) - for supplementing characters defined in the Big5 or ISO 10646 standard<br>• Data messages (e.g. XML messages) encoded in ISO 10646 should adopt UTF-8 as the encoding standard unless the Government specifies otherwise | ✓<br>✓<br>✓<br>✓<br>✓ |

| Interoperability area | Recommended specification(s) | Specification(s) relevant to submissions under ETO |
|---|---|---|
| Compressed files | • .zip<br>• .gz v4.3 | ✓<br>✓ |
| Animation | • Macromedia Flash (.swf)<br>• Apple Quicktime(.qt, .mov, .avi)<br>• Macromedia Shockwave (.swf) | ×<br>×<br>× |
| Moving image and audio/visual | • MPEG-1 (ISO 11172) | × |
| Audio/video streaming | • RealAudio / RealVideo (.ra, .ram, .rm, rmm)<br>• Microsoft MediaPlayer (.asf, .wma, .wmv) | ×<br>× |
| Geospatial data in Planning, Lands & Works | • To be advised by the Housing, Planning and Lands Bureau | To be determined |
| CAD information interchange for the construction industry | • In accordance with the "CAD Standard for Works Departments" to be issued by the Environment, Transport and Works Bureau | ✓ |
| System and data modelling | • UML 1.4 | × |
| Default document/message formatting language | • XML v1.0 | Business specific XML schemas will be published where relevant |
| Default schema definition | • XML Schema 1.0 – for data-oriented message exchange and processing<br>• DTD as defined by XML v1.0 – for document-oriented applications | Business specific XML schemas will be published where relevant |
| Transformation/ Transcoding | • XSL v1.0 | × |

## 7.5 DOMAIN 4: SECURITY

| Interoperability area | Recommended specification(s) | Specification(s) relevant to submissions under ETO |
|---|---|---|
| E-mail security | • S/MIME v2 | ✓ |
| IP network-level security | • IPsec | × |

| Interoperability area | Recommended specification(s) | Specification(s) relevant to submissions under ETO |
|---|---|---|
| IP network-level encryption | • IP ESP | × |
| Transport-level security | • SSL v3.0<br>• TLS v1.0 | ×<br>× |
| Symmetric encryption algorithms | • DES<br>• 3DES – comparatively harder to break | ×<br>× |
| Asymmetric encryption algorithms | • RSA | × |
| Digital signature algorithms | • DSA<br>• RSA for Digital Signatures | ×<br>× |
| Hashing algorithms for digital signature | • SHA-1 | × |
| Cryptographic message syntax | • PKCS #7 v1.5 (RFC 2315) | ✓ |
| On-line certificate status protocol | • RFC 2560 | × |
| Certification request | • RSA PKCS #10 v1.7 (RFC 2986) | × |
| Certificate profile | • RFC 3280 (X.509 v3) | × |
| Certificate revocation list profile | • RFC 3280 (X.509 v2) | × |
| Certificate import/export interface | • PKCS #12 v1.0 | × |
| Cryptographic token interface | • PKCS #11 v2.11 – for non-Microsoft products<br>• Microsoft CryptoAPI – for Microsoft products | ×<br>× |
| Cryptographic token information syntax | • PKCS #15 v1.1 | × |
| 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 |
| Privacy policy | • P3P v1.0 | × |

## 7.6 DOMAIN 5: INTERCONNECTION

| Interoperability area | Recommended specification(s) | Specification(s) relevant to submissions under ETO |
|---|---|---|
| E-mail transport | • SMTP (RFCs 2821, 2822) – for transporting email messages<br>And<br>• MIME (RFCs 2045, 2046, 2047, 2048, 2049, 2231, 3023, 2557, 2392, 2387 ) – for the exchange of complex message types | ✓<br><br>✓ |
| Mail box access | • POP3 - for basic mail box access<br>• IMAP4 rev1 - for more advanced functionality allowing clients to manipulate messages on the server | ×<br>× |
| Hypertext transfer protocol | • HTTP v1.1 | × |
| Directory access | • LDAP v3 | × |
| Domain name service | • DNS | × |
| File transfer | • FTP | × |
| LAN/WAN interworking | • IPv4 | × |
| Transport | • TCP – preferred transport protocol<br>• UDP – where required e.g. to support particular protocols | ×<br>× |
| Wireless LAN | • IEEE 802.11b (subject to security constraints) | × |
| Mobile device Internet access | • WAP v1.2 | × |

# 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), Central Services (CSs) 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 between non-Government networks and the Government network will be addressed on a case-by-case basis and are not addressed here.

## 8.2 MAJOR COMPONENTS OF THE GNA

The GNA defines the relationships between 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 Central Services via these connection points. B/Ds can also make use of the GNET to establish communication channels with other departments.

### B. Government-wide Central Services (CSs)

Central Services are infrastructure components that provide shared Government-wide services, for use by B/Ds. All B/Ds can access Central 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 DNs and CSs. Currently, it consists of a number of routers and switches located in the ITSD Central Computer Centres and various Government buildings.

## 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 Central 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 Central 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 three core components.

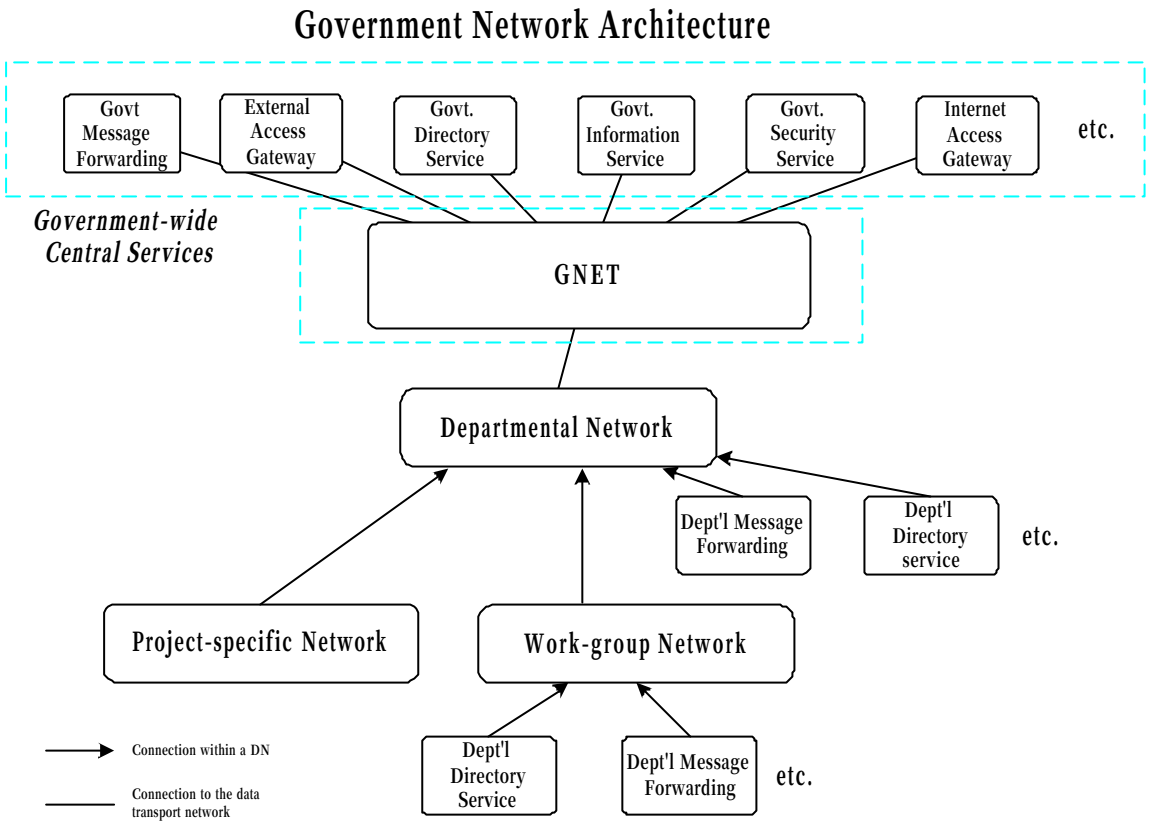


***Diagram 8.1 – The Government Network Architecture***

## 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 DNs and the GNET.

Each DN/CS is defined as an Autonomous System (AS) and is given a unique AS number in accordance with the ITSD 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 DNs, the GNET and the CSs 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);
- IEEE 802.2 (Logical Link Control Interface);
- 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, IEEE 802.2, Frame Relay and AAL5 |

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