The HKSARG Interoperability Framework

Version : 1.0

November 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
	Updates to the consultation draft issued on 30 .7.2002		1.0	Nov 2002
1.	Stronger tone adopted for compliance in Executive Summary and Section 5.2	1-1, 5-1		
2.	Clarified responsibility for on-going management of business/application specific schema in Section 4.3	4-2		
3.	Updated XMLCG terms of reference and immediate work plans	4-2		
4.	Removed reference to ITSD homepage with respect to the publishing of schemas to allow more flexibility as to where the schemas will be published on the Internet	4-4		
5.	Section 5.1 updated to note that individual systems may offer additional system interfaces on top of the basic requirements specified in the Interoperability Framework	5-1		
6.	Section 5.2 updated to reflect correct title for Secretary for Commerce, Industry and Technology	5-2		
7.	Explanation of why cost benefit analysis is required added to Section 5.3	5-2		
8.	Compliance policy elaborated in section 5.3 regarding new versions of the Interoperability Framework	5-2		
9.	Section 5.3 clarification provided on the way to seek additional funding should a cost/benefit analysis determine that a system under development should be aligned with the latest version of the Interoperability Framework.	5-2		
10.	Emphasised role and requirements of project managers in complying with the Interoperability Framework in Section 5.4	5-3		

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
11.	Procurement officers removed from the list of people who need to understand compliance in Section 5.4 because the project officer preparing the tender document should be the one to specify the requirement of particular products and services and to perform tender evaluation	5-3		
12.	Emphasised the need for Heads of ITMUs to approve exemption explicitly in Section 5.6, and to use their professional judgement in approving exemptions.	5-3		
13.	Statement included in Section 5.6 that identical exemptions need to be justified and notified once only.	5-3		
14.	First sub bullet of Area principle (e) modified to include removable storage media	6-1		
15.	Additional principle (f) for selection of Interoperability Areas included	6-1		
16.	Additional principle (k) for selection of Technical Specifications included	6-2		
17.	Backward compatibility addressed as a principle for selecting technical specifications (q)	6-3		
18.	Title of Section 7.1 revised	7-1		
19.	Meaning of multiple standards in one Area clarified	Through-out section 7		
20.	Section 7.1 and 7.2. Business specific domain elaborated to cover other specifications required to enable joined-up services (in addition to data schemas)	7-1, 7-2		
21.	Paragraph inserted under Section 7.2 regarding industry standards adopted by some B/Ds	7-2		
22.	Title for Area intra-government remote service delivery protocol amended (section 7.3)	7-2		
23.	Reference to W3C WAI guidelines added for web page design (section 7.4)	7-3		
24.	Content Publishing area has been renamed as Content Publishing for Document Exchange in Section 7.4	7-3		

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
25.	Elaboration provided as to what is meant by 97 file format for Microsoft software, Section 7.4.	7-3, 7-4		
26.	Graphical / still image file types renamed as Graphical / image file types (section 7.4)	7-5		
27.	EPSF and PNG added as recommended standards for image file types in Section 7.4	7-5		
28.	ISO-8859-1 added as recommended standards in Section 7.4	7-6		
29.	EBCDIC added as a specification for mainframe to mainframe communication Section 7.4.	7-6		
30.	New Interoperability Area added for Removable Storage Media under Section 7.4	7-6		
31.	MP3 added as specification for audio/visual	7-7		
32.	CAD specification renamed to reflect the standard issued by Environment, Transport and Works Bureau	7-7		
33.	Area for system and data modeling removed	7-7		
34.	Area IP network level encryption removed from Domain 4, Security	7-8		
35.	E-mail format added as a new area. Notes RPC added to E-mail transport; MIME transferred to e-mail format, Notes RTF added to e-mail format.	7-9, 7-10		
36.	Clarification provided that TCP is preferred over UDP in Section 7.6	7-10		
37.	For specifications intended to be relevant for submissions under the ETO but are not reflected in the prevailing Format and Manner Requirements, replace the 'tick' with appropriate notes explaining the impact.	Through-out section 7		

TABLE OF CONTENTS

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 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 Interoperability Framework. E-Government applications that depend on, or communicate with those infrastructure systems are therefore required to 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 are required to 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 must 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;
- 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)
Information Technology Services Department

Email: ifcg@itsd.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 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 central 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 mean extra

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

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 respective business application owners and the **XML Co-ordination Group**. 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 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 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 some B/Ds are taking the lead in developing interoperability standards for their respective industries (e.g. Computer-Aided-Drafting Standard for Works Projects). 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 and maintained 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. The maintenance of project defined or business specific schemas should be treated as an integral part of the maintenance of those systems the schemas are designed to serve.

Given the strategic nature of the initiative, and the need for a consistent approach, an XML Co-ordination Group (XMLCG) has been 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 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 Director of Information Technology Services and consists of experienced XML adopters in the public or private sector. In particular, B/Ds that participate in industry led XML initiatives will be invited to join the XMLCG.

To start with, the XMLCG will:

- Develop guidelines for designing and managing XML schemas for e-Government services;
- Progressively develop standard schemas for data items commonly used in e-Government services (core schemas);
- Put in place a registry to facilitate the sharing of information to enable the development of joined-up services and set principles for the use of the registry.

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 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 Internet where relevant.

5. COMPLIANCE

5.1 THE USE OF TECHNICAL SPECIFICATIONS AND PUBLISHED CORE XML SCHEMAS

Compliance with the Interoperability Framework 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 core XML schemas, plus the infrastructure architecture, conventions and procedures specifications listed in the Interoperability Framework document registry, where these exist and where applicable. For new systems where existing technical specifications or core schemas do not address interoperability requirements, a request for change should be raised.

The Interoperability Framework 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 Interoperability Framework. E-Government applications that depend on or communicate with those infrastructure systems are required therefore to comply with the Interoperability Framework to facilitate better integration.

It is strongly recommended that all other new systems (for example, intra-B/D 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 are required to 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 must 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 or systems of external parties. In such cases, compliance with the Interoperability Framework must 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 are required to adopt the core schemas, where relevant, as far as possible.

Although the recommended technical specifications are provided only as a reference 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 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 fulfill B/Ds' operational need, through gazette notices to be issued in relation to Format and Manner Requirements issued by the Secretary for Commerce, Industry and Technology pursuant to the ETO.

5.3 COMPLYING TO NEW VERSIONS OF THE INTEROPERABILITY FRAMEWORK

New integration projects should comply with the version of the Interoperability Framework effective on the date the project seeks endorsement for project implementation. If the version of the Interoperability Framework 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 Interoperability Framework.

The same principle applies when the Interoperability Framework 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 Interoperability Framework.

In certain circumstances, the benefits of compliance with the updated Interoperability Framework 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 Interoperability Framework due to budget, time, and contractual constraints, in which case it would not be appropriate to comply with the updated Interoperability Framework. 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 Interoperability Framework impacts on their project under development.

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 Interoperability Framework and additional cost will be incurred. If the cost/benefit analysis determines that compliance to the updated version is not justified, then the Head of the IT Management Unit (or its equivalent) must approve the result of the cost/benefit analysis.

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 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 Interoperability Framework at external system interfaces;
- Head of the IT Management Units (or its equivalent) in B/Ds – need a thorough understanding of the Interoperability Framework 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 Interoperability Framework 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 ITSD), and report approved exemptions to the IFCG. They must also report on compliance with the Interoperability Framework when completing post-implementation departmental returns;
- Application developers - need a thorough understanding of the Interoperability Framework to adopt relevant specifications as directed during system design and development;
- Project approval authorities - need to understand the Interoperability Framework compliance policy and ensure that Interoperability Framework 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 Interoperability Framework to ensure that solutions proposed to Government comply with the Interoperability Framework where appropriate;
- Project auditors and reviewers - need a high-level understanding of the Interoperability Framework to ensure that Interoperability Framework 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 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 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 Interoperability Framework, 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 ITSD.

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.

Under certain circumstances, B/Ds may be required to seek approval for exemption from compliance because their systems need to comply with industry standards (such as those issued by the International Civil Aviation Organization) 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 standard.

Although compliance to the Interoperability Framework 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;
- new Government to public integration or inter-B/D integration initiatives based on existing systems.

Such reports will help the IFCG assess and improve as soon as practicable the applicability and effectiveness of the Interoperability Framework, 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.

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.
   - 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 secured communication between two parties as required.
f. 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: 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:

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

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:

l. 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.;

m. 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;

n. 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;

o. 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;

p. 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;

q. 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. 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. 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 OVERVIEW

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

- Business specific – business process interaction model, business vocabulary, 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.

In some cases, more than one specification is recommended for an interoperability area. If the recommended specifications functionally serve a different purpose (e.g.WML for use with WAP devices and HTML for use with mini-browsers), the Interoperability Framework will state and differentiate the purpose of the recommended specifications. If the recommended specifications functionally serve the same purpose (e.g. both PKCS #11 and Microsoft CryptoAPI are for interfacing with cryptographic tokens), then the general rule is that the receiver (or responder or server) must support all recommended specifications while the sender (or initiator or requester) may choose to use any of the recommended specifications, unless otherwise specified.

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

7.2 DOMAIN 1: BUSINESS SPECIFIC

In the business specific domain, we focus on business aspects such as:

- how related business processes may interact with each other to provide joined-up services;
- business vocabularies;
- what information is exchanged between interacting applications;
- schemas for business specific data items and data items commonly used in e-government services.

The XMLCG is developing an XML schema design and management guideline which will provide project teams guidance on how to derive and document the above. In addition, the XMLCG will progressively define vocabulary and schemas for data items commonly used in e-government services (referred hereafter as core schemas). The core schemas and project defined process models, schemas, etc. will be posted in a registry for future sharing among stakeholders.

With regard to message formats for data interchange between applications, XML should be adopted for new implementations.

Industry schemas that a number of B/Ds have already adopted as a basis for developing their business specific schemas include NewsML, for the creation, transfer and delivery of news.

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)**	**Is the specification relevant to submissions under ETO ?**
Intra-government remote service delivery protocol (for simple functional integration in a heterogeneous computing environment)	• SOAP v1.1	×
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)**	**Is the specification relevant to submissions under ETO ?**

Interoperability area	Recommended specification(s)	Is the specification 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 (http://www.info.gov.hk/digital21/eng/knowledge/guide/), taking into account the W3C's Web Accessibility Initiative (http://www.w3.org/WAI).	×
Speech	• VoiceXML 1.0	×
Mobile device content	• WML v1.2 – for use with WAP devices • HTML as implemented by commonly adopted browsers on mobile devices - for use with mini-browsers	× ×
Content publishing for document exchange	• Those parts of htm(l) commonly implemented by Netscape Navigator v4.7x and Microsoft Internet Explorer v5.x • PDF v3, 4 or 5 While the sender may choose to use any of the above formats, the receiver must support all of the above formats.	see Note 1 see Note 1

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
Document file types	• .txt	✓
	• .rtf v1.6	see Note 1
	• See Content publishing for document exchange specifications	✓
	While the sender may choose to use any of the above formats, the receiver must support all of the above formats.	
	In addition, B/Ds may, upon the interacting parties' agreement, use any of the following formats for intra-government document exchange	
	• .doc (Word 97 file format) – for exchange between Microsoft Word users (note that 97 is the file format, and not product version that is recommended. Later versions that support this format may therefore be used)	×
	• .sxw – for exchange between users of OpenOffice suite	×
Presentation file types	• see Content publishing for document exchange specifications	✓
	In addition, B/Ds may, upon the interacting parties' agreement, use any of the following formats for intra-government exchange of presentation files	
	• .ppt (PowerPoint 97 file format) – for exchange between Microsoft PowerPoint users (note that 97 is the file format, and not product version that is recommended. Later versions that support this format may therefore be used)	×
	• .sxi – for exchange between users of OpenOffice suite	×

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
Spreadsheet file types	• See Content publishing for document exchange specifications	✓
	In addition, B/Ds may, upon the interacting parties' agreement, use any of the following formats for intra-government exchange of spreadsheet files	
	• .csv – for plain tabulated data	×
	• .xls (Excel 97 file format) – for exchange between Microsoft Excel users (note that 97 is the file format, and not product version that is recommended. Later versions that support this format may therefore be used)	×
	• .sxc – for exchange between users of OpenOffice suite	×
Graphical / Image File Types	• .jpg – for images that will tolerate information loss	✓
	• .gif v89a - for images that will tolerate information loss with few colours and limited graduation between colours	✓
	• .tif v6 - good for images that will not tolerate information loss	✓
	• png v1 – as an alternative to gif v89a offering greater compression and where control over transparency is required	see Note 2
	• epsf v3 – for images that require editing and/or which are included in PostScript printed output	✓
	The choice of specification largely depends on the tool used to generate the image. While the sender may choose to use any of the above formats, the receiver must support all of the above formats.	

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
Character sets and encoding	• ASCII – for encoding content in English	✓
	• BIG-5 – for encoding content in Chinese	✓
	• 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). Data messages (e.g. XML messages) encoded in ISO 10646 should adopt UTF-8 as the encoding standard unless the Government specifies otherwise	see Note 1
	• HKSCS (issued in 1999) - for supplementing characters defined in the Big5 or ISO 10646 standard	✓
	• ISO 8859-1:1998 - an alternative for English language web site content	×
	• EBCDIC – for mainframe to mainframe information interchange	×
	For electronic submission under the ETO : - the sender may use ASCII or ISO 10646 to encode content in English, the receiving B/D must support both ASCII and ISO 10646 - similarly, the sender may use BIG-5 or ISO 10646 to encode content in Chinese, the receiving B/D must support both BIG-5 and ISO 10646	
Compressed files	• .zip	see Note 2
	• .gz v4.3	see Note 2
	While the sender may choose to use any of the above formats, the receiver must support all of the above formats.	

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
Removable storage media	• 3.5" 1.44 MB floppy diskette in MS-DOS format • CD-ROM in ISO 9660:1988 format While the sender may choose to use any of the above media & formats, the receiver must support all of the above media & formats.	✓ ✓
Animation	• Macromedia Flash (.swf) • Apple Quicktime(.qt, .mov, .avi) • Macromedia Shockwave (.swf) The content provider may use any of the above formats, but should ensure that appropriate viewers are openly accessible to the consumer (e.g. as freeware downloadable from the Internet), and provide a pointer to the viewer as necessary	× × ×
Moving image and audio/visual	• MPEG-1 (ISO 11172) - for audio and video • .mp3 (ISO 11172) - for audio	× ×
Audio/video streaming	• RealAudio / RealVideo (.ra, .ram, .rm, rmm) • Microsoft MediaPlayer (.asf, .wma, .wmv) The content provider may use any of the above formats, but should ensure that appropriate viewers are openly accessible to the consumer (e.g. as freeware downloadable from the Internet), and provide a pointer to the viewer as necessary	× ×
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 Projects" issued by the Environment, Transport and Works Bureau	see Note 2
Default document/message formatting language	• XML v1.0	Business specific XML schemas will be published where relevant

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
Default schema definition	• XML Schema 1.0 – for data-oriented message exchange and processing • 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	×

Note 1: There is some difference between the recommended specification and the format stated in the prevailing Format and Manner Requirements. The recommended specification is intended to be relevant for electronic submission under the ETO and will be promulgated to the public through future gazette notices in relation to the Format and Manner Requirements.

Note 2: The recommended specification is intended to be relevant for electronic submission under the ETO and will be promulgated to the public through future gazette notices in relation to the Format and Manner Requirements.

7.5 DOMAIN 4: SECURITY

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
E-mail security	• S/MIME v2	✓
IP network-level security	• IPsec	×
Transport-level security	• SSL v3.0 • TLS v1.0 The initiator may use either SSL or TLS. The responder must support TLS which is backwardly compatible with SSL.	× ×
Symmetric encryption algorithms	• DES • 3DES – comparatively harder to break The choice of algorithms depends on the level of security required	× ×

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
Asymmetric encryption algorithms	• RSA	×
Digital signature algorithms	• DSA • RSA for Digital Signatures The sender may use either of the above algorithms. The receiver must support both algorithms	× ×
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	Cryptographic tokens not dedicated for a specific purpose need to support all of the following interfaces • PKCS #11 v2.11 • Microsoft CryptoAPI Applications that use tokens may choose to use either of the above interfaces	 × ×
Cryptographic token information syntax	• PKCS #15 v1.1	×
XML message encryption	• XML Encryption	To be specified along with the business specific XML schema

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
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)	Is the specification relevant to submissions under ETO ?
E-mail transport	• SMTP (RFCs 2821, 2822) – for e-mail exchange through the Internet • Notes Remote Procedure Call - for e-mail exchange through the Government Communication Network (GCN)	see Note 1 ×
E-mail format	• MIME (RFCs 2045, 2046, 2047, 2048, 2049, 2231, 3023, 2557, 2392, 2387) - for e-mail exchange through Internet and for e-mail exchange between the Government Communication Network (GCN) Internet mail gateway and B/Ds using Notes R5 • Notes Rich Text Format - for internal e-mail exchange through the GCN and for e-mail exchange between the GCN Internet mail gateway and B/Ds using Notes R4	see Note 2 ×
Mail box access	• POP3 - for basic mail box access • IMAP4 rev1 - for more advanced functionality allowing clients to manipulate messages on the server	× ×
Hypertext transfer protocol	• HTTP v1.1	×
Directory access	• LDAP v3	×
Domain name service	• DNS	×

Interoperability area	Recommended specification(s)	Is the specification relevant to submissions under ETO ?
File transfer	• FTP	×
LAN/WAN interworking	• IPv4	×
Transport	• TCP – preferred transport protocol over UDP • UDP – where required e.g. to support particular protocols	× ×
Wireless LAN	• IEEE 802.11b (subject to security constraints)	×
Mobile device Internet access	• WAP v1.2	×

Note 1: There is some difference between the recommended specification and the format stated in the prevailing Format and Manner Requirements. The recommended specification is intended to be relevant for electronic submission under the ETO and will be promulgated to the public through future gazette notices in relation to the Format and Manner Requirements.

Note 2: The recommended specification is intended to be relevant for electronic submission under the ETO and will be promulgated to the public through future gazette notices in relation to the Format and Manner Requirements.

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.

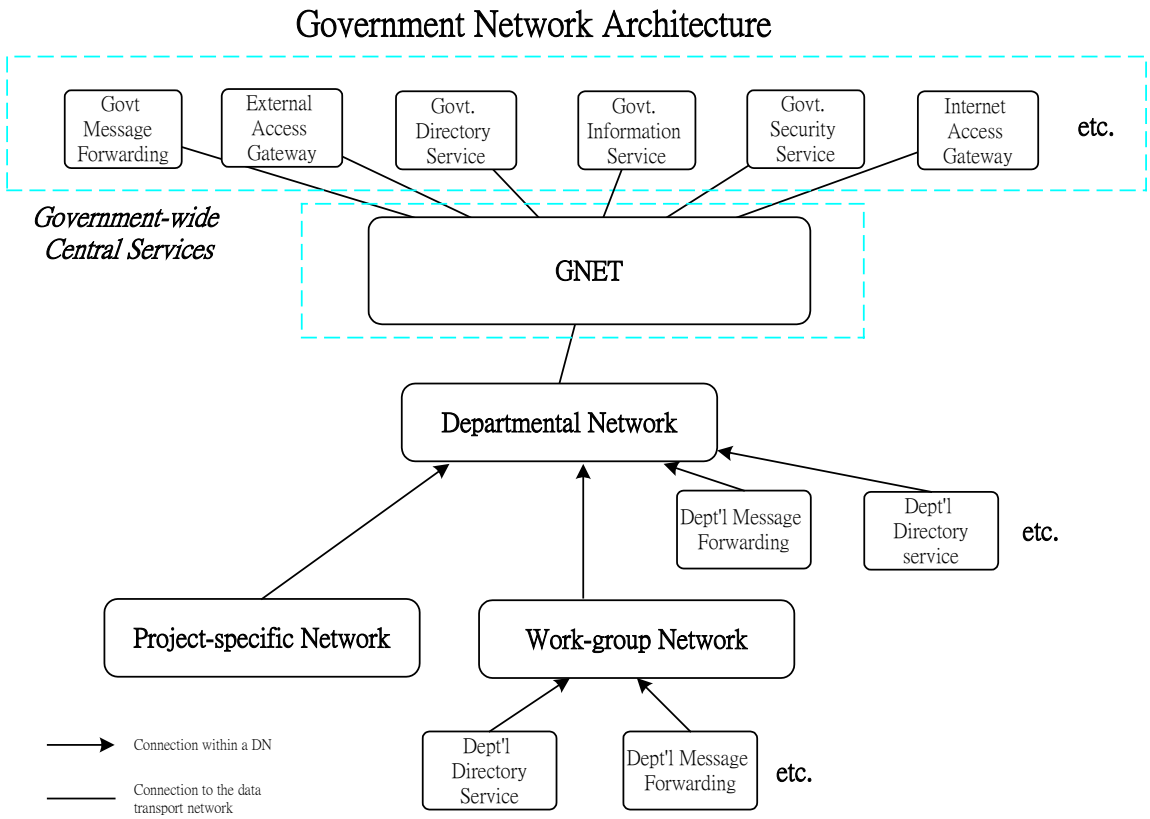

Diagram 8.1 – The Government Network Architecture

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

9. ABBREVIATIONS AND ACRONYMS

3DES	Treble Data Encryption Standard
3G	Third Generation mobile phones
AAL5	Asynchronous Transfer Mode Adaptation Layer Type 5
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
BIG-5	The Standard for the Coding of Chinese Characters Promulgated by the Institute for Information Industry of Taiwan
BGP	Border Gateway Protocol
B/D	Bureau/Department
CAD	Computer-Aided-Drafting
CIG	Central Internet Gateway
CS	Central Service
DES	Data Encryption Standard
DN	Departmental Network
DNS	Domain name services
DSA	Digital Signature Algorithm
DTD	Document Type Definition
EBCDIC	Extended Binary-Coded Decimal Interchange
ECMA	European Computer Manufactures Association
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	Hypertext Markup Language
HTTP	Hypertext transfer protocols
ICMP	Internet Control Message Protocol
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
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO/IEC	International Standards Organization
ITG InfoStation	IT in Government Information Station
ITMU	IT Management Unit
ITSD	Information Technology Services Department

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MS-DOS	Microsoft Disk Operating System
OSPF	Open Shortest Path First
P3P	Platform for Privacy Preferences Project
PDF	Portable Document Format
PKCS	Public Key Cryptography Standards
POP	Post Office Protocol
RC4	Rivest's Cipher 4
RFC	Request for Comments
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm 1
SMTP	Simple Message Transfer Protocol
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
S/MIME	Secure Multipurpose Internet Mail Extensions
TAIGA	Technical Architecture for I-Net Government Applications
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
VoiceXML	Voice Extensible Markup Language
W3C	World Wide Web Consortium
WAE	Wireless Application Environment
WAI	Web Accessibility Initiative
WAN	Wide Area Network
WAP	Wireless Application Protocol
WML	Wireless Markup Language
XML	Extensible Markup Language
XMLCG	XML Co-ordination Group
XSL	Extensible Stylesheet Language