TECHNICAL ARCHITECTURE FOR I-NET GOVERNMENT APPLICATIONS (TAIGA)

[S16]

Version : 1.2

Feburary 2000

TABLE OF CONTENTS

1. PURPOSE

The purpose of this document is to provide guidelines and a technical framework for developing Internet technology-based applications. The guidelines and technical framework adopted are based on the recommendations of the Internet Study on Technical and Legal Issues commissioned by the Task Force on Exploiting Internet Technologies for Government. The guidelines and technical frameworks apply to both Internet and Intranet (I-Net) applications.

The Technical Architecture for I-Net Government Applications, TAIGA in short, provides a technical framework to understanding the relevance of Internet technology to the development of Government applications. It serves as a reference model to facilitate I-Net project planning, scope setting, development, evolution and support.

2. SCOPE

This document explains the Technical Architecture for I-Net Government Applications (TAIGA) and discusses Internet security, legal, and privacy issues of developing I-Net applications.

The technical architecture should serve as the basic reference for bureaux / departments venturing into Internet and Intranet applications. The approved architecture should be followed in developing Internet and Intranet projects for the Government of the Hong Kong Special Administrative Region.

3. REFERENCES

3.1 STANDARDS

- [G3] Guidelines on I.T. Security, Version 3.0, September 1998
- [G4] Guidelines on Micro-computer and LAN Security, December 1995
- [G35] ITSD LAN Address & Naming Standard, August 1993
- [S10] Chinese Standard for Government IT Applications, May 1992
- [S15] Government Systems Architecture, December 1996

3.2 OTHER REFERENCES

- [1] Internet Study Technical and Legal Issues, Version 1.2, 17 October 1997
- [2] Internet Study Standard and Guidelines, November 1997
- [3] Internet Service Acceptable Use Guidelines, ITSD Circular No. 10/96, 8 Nov. 1996
- [4] Situation Paper on Common Person-related Data Definition, Common Person-related Data Definition Task Force, ITSD, March 1992.
- [5] Personal Data Privacy and the Internet – A Guide for Data Users, Privacy Commissioner's Office, December 1997
- [6] Internet Surfing with Privacy in Mind – A Guide for Individual Net Users, Privacy Commissioner's Office, December 1997
- [7] Code of Practice on the Identity Card Number and other Personal Identifiers, Privacy Commissioner's Office, January 1998
- [8] Preparing On-line Personal Information Collection (PIC) Statement and Privacy Policy (PPS) Statement, Privacy Commissioner's Office, December 1998
- [9] Technical position paper on Secured Firewall System, ITSD, June 1998
- [10] RFC 1594: FYI on Questions and Answers - Answers to Commonly asked "New Internet User" Questions
- [11] Web Content Accessibility Guidelines 1.0, W3C, 5 May 1999
- [12] Digital 21 IT Strategy Initiatives - Chinese Language Interface
- [13] Electronic Transactions Ordinance (Cap. 553)

- [14] Code of Practice for Recognised Certification Authorities, ITSD, January 2000

4. DEFINITIONS AND CONVENTIONS

4.1 DEFINITIONS

Terms	*Definition*
BOOTP	Bootstrap Protocol (BOOTP) is a protocol that enables machine on a network to discover its own network IP address, the IP address of a BOOTP server on the network, and a file to be loaded into the machine's memory to boot the machine. The network administer could preset the BOOTP server to automatically assign the IP address from a pool of addresses. The protocol is specified in RFC 951.
CGI	The common gateway interface (CGI) is a specification for passing control and transferring data between World Wide Web server and an application program (CGI program). CGI programs are the common way for Web servers to interact with users. A CGI program could be written in C, Perl, Java, or Visual Basic. Many HTML pages that contain forms, for example, use a CGI program to process the form's data once received by the Web server. The method or convention for passing data back and forth between the server and the application is called the common gateway interface (CGI). One problem with CGI is that each time a CGI script is executed, a new process is started. This can slow down a busy Web server noticeably.
CORBA	Common Object Request Broker Architecture (CORBA) is an architecture and specification for creating, distributing, and managing distributed program objects in a network. CORBA was developed by an industry consortium known as the Object Management Group (OMG). OMG currently includes over 500 member companies. Both International Organization for Standardization (ISO) and X/Open have approved CORBA as the standard architecture for distributed components. The major competing model is Microsoft's COM and DCOM.

Terms	*Definition*
DCOM	Distributed Component Object Model (DCOM), an extension of Component Object Model (COM), is the Microsoft's implementation to support objects distributed in a network. For instance, a client program object can request services from server program object residing on other computers in a network. Until recently, DCOM is implemented only on Windows platform.
DES	Data Encryption Standard (DES) is a popular symmetric-key encryption method developed in 1975 and endorsed by the US government in 1977. DES was accepted as ANSI Standard X.3.92 in 1981 and widely adopted by the US government. As DES is a symmetric cryptosystem, both sender and receiver must know the same secret key to encrypt and decrypt the messages. In a multi-user environment, the distribution of such secret key may be difficult in contrast with the public key cryptography. The DES has a 64-bit block size and uses a 56-bit key during encryption, whereas 3DES uses 128 bits key.
DHCP	Dynamic Host Configuration Protocol (DHCP) is a client/server based protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. Dynamic addressing simplifies network administration because the software will keep tracks of IP addresses rather than requiring an administrator to manage the task for every device.
Firewall	Firewall is a system designed to prevent unauthorised access to or from a private network. All messages entering or leaving the internal private network must pass through the firewall, which filters and blocks the passage based on user-defined rules (security policy).

Terms	*Definition*
GCCS	The Government Chinese Character Set (GCCS) is a set of user-defined characters defined by the HKSAR Government. The software files for the character set are now made available to the public who may use it with Microsoft Chinese Windows (BIG-5). Only Chinese characters commonly used in office automation environment are covered by GCCS. In September, 1999, GCCS is enhanced and known as HKSCS.
HKSCS	The Hong Kong Supplementary Character Set (HKSCS) is an updated version of the Government Chinese Character Set (GCCS) co-developed by ITSD and Official Languages Agency (OLA), in consultation with Chinese Language Interface Advisory Committee (CLIAC), which has been released in September, 1999. The HKSCS, as a supplementary character set of the Big-5 and ISO 10646 coding schemes, contains Chinese characters needed in Chinese computing in Hong Kong but are not contained in either the Big-5 or ISO 10646 standard character set.
HTML	The HyperText Markup Language (HTML) is a W3C language standard used for publishing information in the World Wide Web system. Current HTML version supports the following: ● Publish online documents with headings, text, tables, lists, photos, etc. ● Retrieve online information via hypertext links, at the click of a button. ● Design forms for conducting transactions with remote services, for use in searching for information, making reservations, ordering products, etc. ● Include spreadsheets, video clips, sound clips, and other applications directly in their documents.
HTTP	The Hyper Text Transfer Protocol (HTTP) is the underlying protocol used by the World Wide Web. The protocol defines how messages are formatted and transmitted, and the commands used by the Web servers and browsers.

Terms	*Definition*
IETF	The Internet Engineering Task Force (IETF) is the standards organisation that defines protocols, development and standards for the Internet on an operational level.
IMAP4	Internet Message Access Protocol (IMAP) is a standard protocol for retrieving e-mail messages from mail server. The latest version, IMAP4, is a client-server protocol supporting users to read the message header information while the messages are still on the mail server. User can selectively download the e-mail messages for reading. User can also create and manipulate folders or messages on the server, or search for certain parts or an entire note. However, IMAP requires connection to the server during the entire session when e-mail messages are being manipulated on the mail server. In contrasts with POP3 protocol, the e-mail clients need to download the e-mail messages to the local machine in batch for off-line reading.
ISO 10646	The ISO 10646 is the standard dealing with issues of the representation of international characters, text direction, punctuation, and world language issues. As one of the initiatives in Digital 21 IT Strategy, ISO 10646 is embraced to be adopted in the long term as the Chinese character set standard for users who prefer to communicate electronically in Chinese.
Java	Java is a high-level programming language developed by Sun Microsystems for use in the distributed network environment like Internet. Java is basically an object-oriented language similar to C++ language and implemented with an architecture-neutral programming environment. Small Java applications are called Java applets and can be downloaded from a Web server and executed by a Java interpreter and runtime environments, known as Java Virtual Machines, commonly supported by the latest browsers including Netscape Navigator and Microsoft Internet Explorer.

Terms	*Definition*
JavaScript/JScript	JavaScript is an interpreted scripting language developed by Netscape. JavaScript shares many of the features and structure borrowed from Java language but was developed independently. JavaScript is an open language that anyone can use without purchasing a license and is supported by recent browsers from Netscape and Microsoft. JScript is Microsoft's own implementation of JavaScript, which has been built into Internet Explorer browsers.
LDAP	Lightweight Directory Access Protocol (LDAP) is a set of protocols to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate Intranet. LDAP is based on the Directory Access Protocol (DAP) standards contained within the X.500 standard defining directory services in a network but is significantly simpler or "lightweight". LDAP supports TCP/IP and is widely endorsed by at least 40 companies including Netscape, Microsoft and Novell. An LDAP directory is organized in a simple “tree” hierarchy consisting of the “root” directory, Countries, Organizations, Organizational Units (divisions, departments, and so forth), Individuals (which includes people, files, and shared resources such as printers) and can be distributed and replicated among many servers. As LDAP is an open protocol, applications like the Internet e-mailer can easily obtain the directory information from any directory server on the network.
MIME	Multipurpose Internet Mail Extensions (MIME) is a specification for formatting non-ASCII messages so that people can exchange message text in languages with different character sets, and send and receive multimedia file types including audio, video, image, application programs, and others via the Internet mail systems. MIME is specified in RFC 1521.

Terms	*Definition*
NDS	Novell Directory Services (NDS) is the directory services developed by Novell for the NetWare networks. NDS complies with the X.500 standard and provides a logical tree-structure view of all resources on the network. Users can access the resources according to the authorization rights defined by the administrator. NDS for NT allows a NDS user to access the resources in NT servers on the network.
NNTP	Network News Transfer Protocol (NNTP) is the protocol used to post, distribute, and retrieve USENET messages. It specifies how the clients (news reader) view and post messages to a newsgroup which is hosted on a news server on the Internet. The protocol is specified in RFC 977.
ODBC	Open DataBase Connectivity (ODBC) is a standard database access method and open application programming interface (API) for accessing a database developed by Microsoft. Since ODBC version 2.0, the standard supports the Structured Query Language (SQL) Call-Level Interface. ODBC was designed to enable the access of any data from any application, regardless of which database management system is maintaining the data. It allows programs to use SQL requests to access databases without knowing the proprietary interfaces. ODBC would handle the SQL request and converts it into a compatible request for the individual database system.
Perl	The Practical Extraction and Report Language (Perl) is an interpreted scripting, text manipulation language with syntax similar to the C language but includes a number of popular UNIX facilities taken from grep, sed, awk, and tr. Because of its strong text processing abilities, Perl has become one of the popular languages for writing CGI scripts.

Terms	*Definition*
POP3	Post Office Protocol (POP) is the protocol used to retrieve e-mail messages from a mail server. The older version, POP2, became a standard in the mid-80s and requires SMTP to send messages. The POP3 is the most recent version which can be used with or without SMTP for receiving e-mail messages.
RSA	RSA is a public-key cryptosystem invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. They founded the RSA Data Security, Inc. in 1982 and named after their last names. RSA use public-private key pairs for encryption and authentication. Each user uses only other's public key and its own private key. The RSA algorithm is based on the assumption that there is no efficient way to factor very large numbers and it would require a significant amount of computer processing power and time to deduce an RSA key.
S/MIME	Secure/Multipurpose Internet Mail Extensions **(**S/MIME) is a new version of the MIME protocol that supports encryption of messages. S/MIME was designed to support secure messaging by sending digitally signed and encrypted messages to one another. S/MIME v2 requires the use of RSA key exchange, patented by RSA Data Security, Inc.; and weak cryptography (40-bit keys). This prevents the protocol from being accepted as an IETF standard. S/MIME Version 2, is specified in RFC 2311 as Informational. However, S/MIME v2 has been widely endorsed by major networking and messaging vendors including Microsoft, Lotus, Netscape, Novell, and VeriSign in developing secure messaging and related products. S/MIME v3, specified in RFC 2633 as Standard Track, permits the use of variable encryption key lengths up to 128 bits.

Terms	*Definition*
SET	Secure Electronic Transaction (SET) is a new standard that will enable secure credit card transactions on the Internet. The cryptographic protocol was designed to safeguard transmission of sensitive personal and financial information over insecure communication channel. SET has been endorsed by major players in the electronic commerce arena, including Mastercard, Visa, Microsoft, and Netscape.
SMTP	Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. SMTP is also generally used to send messages from a e-mail client to a mail server.
SQL	Structured Query Language (SQL) is a standardised query language for requesting information from and updating information to a database. SQL was designed by an IBM research centre in 1974 and was commercialised by Oracle Corporation in 1979. The ANSI approved a rudimentary version of SQL as the official standard in 1986, but since then vendors have include different extensions to the ANSI standard. ANSI has updated the standard in 1991 and known as SAQ SQL.
SSL	Secure Sockets Layer (SSL) is a protocol developed by Netscape for transmitting data securely over the Internet. SSL provides privacy and reliability between two communicating applications. SSL is application protocol independent and composed of two layers. The lowest layer of SSL, layered on top of transport protocol like TCP, is used for encapsulation of higher level protocols. Such higher level protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives data. By convention, Web pages that require an SSL connection start with https: instead of http:. Both recent browsers from Microsoft and Netscape support SSL.

Terms	*Definition*
SSO	Single Sign On (SSO) gives end-users a single user ID and one password for access to the entire enterprise network resources. SSO must be implemented with strong security features including encryption, authentication, synchronization, and audit trail. An SSO solution normally have to work across different hardware platforms, operating systems, network protocols, application types and causes the administration work complicated. Major software vendor like IBM has solution on SSO but still required the administrator to handle with special care.
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP) is the suite of communication protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones are TCP and IP, which is built into the UNIX operating system and is used by the Internet. TCP/IP is the de facto standard for transmitting data over networks. For other network operating systems such as NetWare, also support TCP/IP in addition to their own protocols.
VBScript	Visual Basic Scripting Edition is a scripting language based on the Visual Basic programming language developed by Microsoft. VBScript is supported by Internet Explorer and enables Web authors to develop interactive Web pages.
X.500	X.500 is an ISO and ITU standard for directory services defining how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as e-mail addresses, postal addresses, telephone, fax and teletext addresses, organizational relationships, graphical data.
X.509	X.509 is an ITU (International Telecommunication Union) recommendation which specifies the authentication service for X.500 directories, as well as the widely adopted X.509 certificate syntax. The initial version of X.509 was published in 1988 and the latest version was proposed in 1994 and considered for approval in 1995.

Terms	*Definition*
XML	The Extensible Markup Language (XML) is developed by an XML Working Group formed under the auspices of the World Wide Web Consortium (W3C) in 1996. It becomes a W3C standard in 1998. Like HTML, the language is optimized for publishing information in the web. Unlike HTML, user can define its own data element in XML specific to the user's business.

4.2 CONVENTIONS

N.A.

5. SUMMARY OF TAIGA

5.1 BACKGROUND ON INTERNET

The Internet is a collection of thousands of networks linked by a common set of technical protocols which make it possible for users of any one of the networks to communicate with or use the services located on any of the other networks. These protocols are referred to as the TCP/IP protocol suite.

The Internet started in the late 1960s as a wide-area network created by the US Defense Advanced Research Projects. The Advanced Research Projects Agency Network (ARPANET), established in 1969, served as a testbed for new networking technologies linking universities and research centers. The ARPANET started with three nodes, the UCLA, the Stanford Research Institute, and the University of Utah. Today, the Internet has included such networks as the National Science Foundation Network (NSFNET), the Australian Academic and Research Network (AARNet), the NASA Science Internet (NSI), the Swiss Academic and Research Network (SWITCH), and over 10,000 other large and small, commercial and research networks. As of June 1998, the Internet has more than 130 million users distributed in over 100 countries, and that number is growing rapidly.

Until the mid-1980s, the Internet was composed mainly of e-mail, file transfer protocol (FTP), remote login (Telnet), and remote document access (Gopher). It was the advent of the World Wide Web (Web) and its related technologies, which has really brought the Internet to public attention. With an estimated number of over 650,000 Web sites available around the world, the Web has become the major growth area and serves as a effective means in delivering electronic information that can integrate both text and multimedia elements like graphics, animation, voice and video.

Using standard Internet technology as its backbone, the Web has become the IT phenomena of the 1990s. With a potential market as large as that of the Internet itself, the Web has become the tool of choice for most organizations to improving service delivery, making contact with clients, and even conducting business. For the HKSAR Government, all Bureaux and Departments had set up Internet presence in 1997. Although the Web pages tend to be relatively static and are generally involve one-way communication with the user, the modern Internet technologies are rapidly advancing to the point where interactive, two-way communication can take place. As such, applications based on modern technology open up the possibility to provide government service and conduct business interactively over the Internet. The edge of these Internet applications are they can be customized to deliver information and services in a non-stop fashion, 24 hours a day and 7 days a week, to users around the world regardless of their physical location.

The Internet is open in the fashion that its structure, regulation, and management are not owned by a single entity. The individual networks that make up the Internet are each owned separately and self-managed. The Internet Service Providers (ISPs) provide connectivity for users or organizations, for a fee and allow their computers and networks to communicate with others. This potential of chaos in such mode of

operation was recognized early on; which led to the formation of the Internet Advisory Board (IAB) in the early 1980s to set standards for the overall technical aspects of the Internet, at an architectural level. The Internet Engineering Task Force (IETF), a collection of sub-committees under the IAB, responsible to define protocols, development and standards on an operational level. Another significant body is the World Wide Web Consortium (W3C) which found in 1994 to lead the Web by developing common protocols that promote its evolution and ensure its interoperability.

5.2 BACKGROUND OF TAIGA

In May 1997, the Task Force on Exploiting Internet Technology for Government endorsed the proposal for conducting a study on Internet technical and legal issues (the Study). The main objectives of the Study are to examine the issues and constraints of Internet applications; and to develop a set of guidelines and standards for broader development of Internet usage within the Government.

The Study was completed in November 1997. It concluded that technologies are available to address the security, legal and payment concerns; and recommended a Technical Architecture for I-Net (Internet and Intranet) Government Applications to serve as a technical framework for developing Internet technology-based applications.

5.3 WHAT IS TAIGA

The goal of the Technical Architecture for I-Net Government Applications (TAIGA) is to maximize the ability of the Government to effectively exploit Internet technologies in the development of Internet and Intranet projects.

TAIGA consists of five layers:

- **Layer five: Application Categories** TAIGA identifies eight categories of I-Net applications, each of which raises distinct issues and places successively greater demands on the underlying frameworks, services, security, and communications.

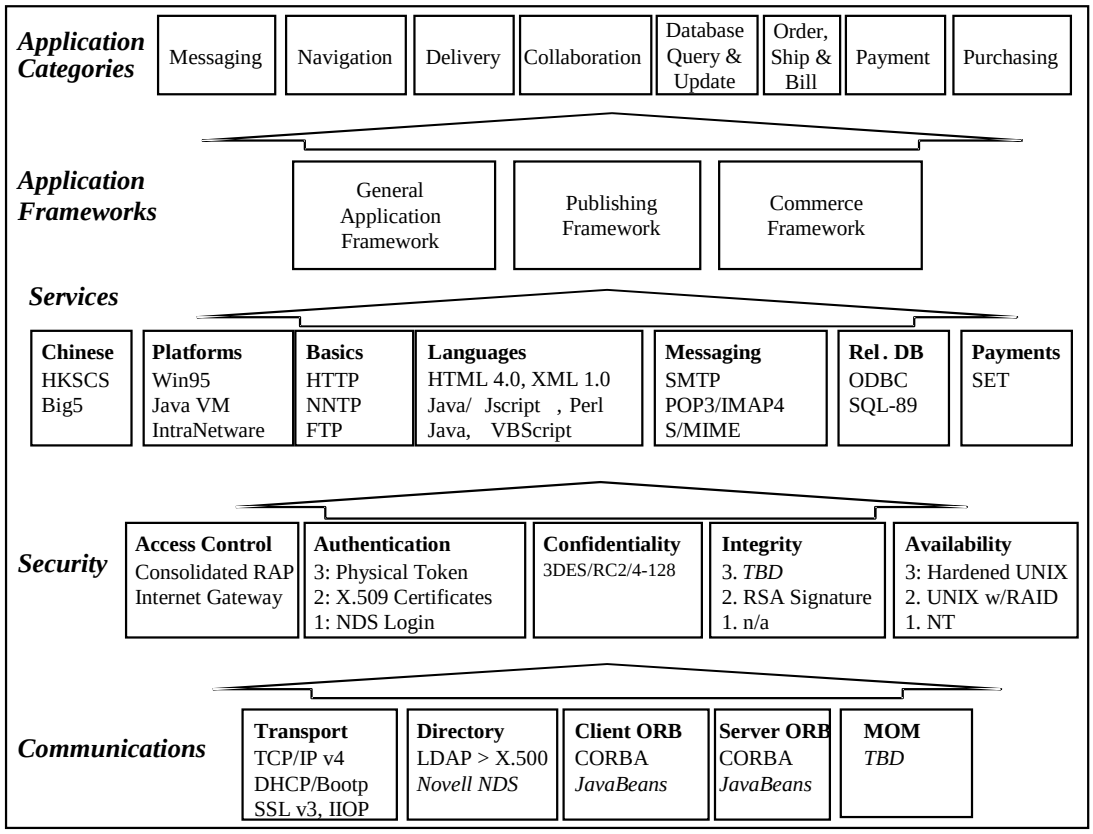
- **Layer four: Application Frameworks** Every major software vendors has an Internet application framework usually addressing the needs of electronic commerce but encompassing languages and development environments, a variety of modular services, standard and proprietary protocols, and differing in their features and functions. TAIGA allows for more than one of these vendors' frameworks to be operational at any given time.

- **Layer Three: Services** The shared services that should be implemented with common interface for providing government-wide I-Net services. These services may include Chinese processing; communication protocols and services such as Internet gateways and directories; data services such as file transfer, distributed session management and transaction processing; and commerce services such as on-line payment.

- **Layer Two: Security** Managing I-Net security is a key focus of TAIGA, since it is the most important building block for I-Net applications. These services cover the areas of confidentiality, authentication, integrity, access control and availability.

- **Layer One: Communications** Network infrastructure encompasses key hardware and OS platforms, network protocols and management, as well as key communications services such as the government-wide directory.

Figure 1 - Recommended standards in TAIGA



Note: Level 3 security is stronger than level 1. TBD means "To be determined"

5.4 KEY ELEMENTS OF TAIGA

TAIGA builds upon existing standards already adopted by the Government, and to augment existing standards that are sufficiently comprehensive with respect to the Internet. One of the key advantages of conformance to Internet standards is the ability to support interoperability among a variety of vendor platforms and to use common architectural elements and servers for both Internet, Intranet, and Extranet applications.

The key elements of TAIGA include :

- *TCP/IP at desktop*, the GNET, with conformance to the Government Network Architecture (GNA), is based on TCP/IP protocol. The extension to use TCP/IP at the desktop level would be a key driver and foundation for a

government-wide Internet/Intranet infrastructure.

- *Common X.500 government hierarchical directory,* provides a global view and administration mechanism for user information and network resources. X.500 standard is comprehensive and highly scaleable yet complex. The Lightweight Directory Access Protocol (LDAP) is a scaled down version of X.500 and is recommended as transitional government-wide and long term departmental directory solution.

- *Use CORBA first and DCOM sparingly,* Object Oriented Broker provides the glue to connect components at different tiers. CORBA provides better cross platform communication in a distributed architecture. DCOM is only acceptable for use if better interactions among Microsoft systems are required.

- *Multi-tiered / loosely-coupled message-based application design,* provides for greater maintainability and centralisation of managing disk storage, compute intensive processing, and network security.

- *Control dial-in, limit dial-out*, the implementation of standardised Internet gateway eliminates the need for individual dial-out access to the Internet. Dial-in should be connected to the government network with strong security monitoring.

- *Standardised Internet gateway*, a secure Internet gateway template is specified in section 6.1.4.3. The template serves as a reference design in implementing Internet connection with centralised point of security control and Internet servers for the deployment of common Internet services.

- *X.509 certificate,* data communications with public key encryption is recommended because it is secure and the key distribution mechanism is scaleable. This will require a trusted third party, called Certificate Authority (CA), to endorse on the authenticity of the public key. Establishing the public CA and using digital certificates in X.509 standard format is critical to the success of electronic commerce.

- *Use UNIX and NT at different tiers,* security and availability favour UNIX as gateway hosts while the lower system cost and wide availability of software solution prefer NT as application servers.

- *Chinese language,* the use of BIG5 encoding scheme supplemented by HKSCS provides a common representation of the traditional Chinese character set for the Chinese community.

- *SMTP, S/MIME based messaging,* electronic message should be coded in MIME format and S/MIME format for end-to-end security and deliver using the SMTP protocol. This unifies the delivery mechanism within and beyond the government networks.

- *Secure Electronic Transaction (SET),* payment over Internet will be done largely using credit cards. SET provides security and authentication to both

the customer and the merchandiser.

- *Standardised searching function*, consistent set of search function among government Web sites enhance the user experience of accessing the vast archive of government data.

- *Standardised content management*, streamlines the publishing cycle of electronic data both within government and to the general public. Template-based publishing tools ensures consistent presentation while content repository at the database increases the reliability.

5.5 TAIGA AND EXISTING STANDARDS

The elements of TAIGA supplement the existing ITSD standards to reflect emerging Internet technology. It supplements and enhances the standards in the area including I.T. Security [G3], LAN Naming and Addressing [G35], Microcomputer and LAN Security [G4], Government Systems Architecture [S15], and Chinese Language [S10].

5.5.1 Guidelines on I.T. Security [G3]

Internet connections to arbitrary Internet Service Provider create security and performance issues. For departmental gateway as well as gateway for the entire Government Communication Network (GCN), TAIGA calls for the use of a template approach for the standard gateway configuration as depicted in 6.1.4.3.

Encryption and the related public key infrastructure are recommended for confidentially and authentication. Their components include use of RSA encryption, National Institute for Standards and Technology (NIST) Digital Signature Standard (DSS), X.509 certificates, Secure Sockets Layers v3 (SSL) and the use of Secure Electronic Transaction (SET).

The continued ability to use data encryption by general public and other external users is recommended in TAIGA, the related legal issues should be exploited when such applications would be developed.

5.5.2 ITSD LAN Naming and Addressing Standard [G35]

The architecture calls for converting from static address to DHCP assigned dynamic Internet Protocol (IP) addressing scheme. To conform to Internet standard, the addressing scheme of the hosts should follow the scheme defined by Internet Assigned Numbers Authority (IANA). Adopting the IANA number for Intranet would prepare a smooth transition to the next version of IP protocol, IPv6.

5.5.3 Guidelines on Microcomputer and LAN Security [G4]

TAIGA recommends for more restrictive use in the areas of dial-in remote access and dial-out Internet access for any departmental LAN having hosts visible outside the gateway. Inbound IP log-in to any departmental LAN via the Internet gateway should not be allowed.

With the secure gateway in place, TAIGA recommends that basic Internet access including SMTP, NNTP, FTP, and HTTP should be routinely granted to the office workers.

5.5.4 Government Systems Architecture [S15]

TCP/IP may be encrypted via Secure Sockets Layer (SSL) to enhance the communication integrity and confidentially. Authentication enhancement is possible via the use of government-wide directory.

I-Net database applications should be constructed using multi-tier loosely coupled topology. TAIGA further elaborates on GSA in the area of client-server middleware. Common Object Request Broker Architecture (CORBA) compliant object request brokers are recommended in most situations. Distributed Component Object Model (DCOM) and ActiveX components may be use where both client and server are limited to Windows platforms.

5.5.5 Chinese Standard for Government IT Applications [S10]

Chinese language content in all eight application categories should be in Traditional Chinese character set using BIG5 encoding scheme supplemented by the HKSCS. I-Net application should also provide expandability option to adopt the ISO 10646 encoding scheme to facilitate an open, common Chinese application interface adopted by the HKSAR. Display of characters based entirely on actual image representation (bitmap) is not recommended due to severe limits in performance and restrictions in the manipulation of data.

5.6 TAIGA AND EXISTING I.T. PROJECTS

Although TAIGA specifies a common Internet architecture to allow projects to proceed in a co-ordinated and efficient manner, this technical architecture does not replace all standards being used in the Government. In particular, implementing TAIGA does not imply that existing systems, organisations, processes and staff must change within any particular time period.

TAIGA does not attempt to homogenise the current IT environment in the Government. It provides a generic architecture for all Internet applications, with the vendors' application frameworks evolving over time as a result of different implementations in various departments.

5.7 TAIGA AND FUTURE I.T. PROJECTS

TAIGA is based on internationally accepted standards and de-facto industry standards, and with updates from experience gained in building I-Net projects. The target is toward the sharing of common technology, technical resources and common services.

The TAIGA architecture should be followed in developing Internet and Intranet applications that would start after the effective date of this document. These applications should be mapped into TAIGA application categories. The corresponding

elements in the four lower layers of architecture, “Application Framework”, “Services”, “Security”, and “Communications” will serve as a base reference to building the applications.

The design of TAIGA applications should focus on the interfaces among standard components. They should aim at delivering logic and contents without creating new unique services.

6. INTERNET ISSUES

6.1 INTERNET SECURITY ISSUES

Internet applications create new demands on the security infrastructure. Specifically, issues related to confidentiality, authentication, integrity and availability have to be addressed.

The section on "Internet Security" in the *Guidelines on Information Technology Security* [G3] should be observed for all I-Net applications.

For unregulated environment like Internet where the user community is open, cryptography is the core technology that can be use to ensure integrity and confidentiality. Using digital signature, the accidental or intentional changes to the original data could be identified.

6.1.1 Confidentiality

Section 10.3 on "Internet Security" in the *Guidelines on Information Technology Security* [G3] has specified the requirement for stronger authentication mechanism and interoperable cryptography mechanisms. This should be implemented using public-key encryption algorithm. The public key encryption algorithm eliminates the complexity of secret keys distribution associated with symmetric-key algorithms but requires a process to ensure authenticity of the public keys.

Except for messaging application that requires S/MIME for end-to-end encryption, Secure Sockets Layer (SSL) v3 may be used to provide secure communications to all application categories at the transport level. SSL allows client/server mutual authentication, integrity using digital signature and privacy through encryption.

The cryptographic keys should have a minimum length of 128 bits. This may require non-US source for encryption software as the current US federal regulation limits the export of strong encryption capabilities, secret keys may not exceed 56 bits key length and public keys used for encryption may not exceed 512 bits.

Products with key escrow may be tolerated until a more permanent solution is available. These products have key length of 56 bits but with the extra part of the key escrowed by US government, making effective key length of more than 56 bits to the world other than the US Government.

6.1.2 Integrity

Use digital signature to ensure integrity of documents. The variation of public key encryption algorithm is used for digital signature. The message digest is produced from the message using a one way hash function. The sender will sign for the validity of the message by encrypting the message digest with his/her private key. The recipient could validate that the message had not been tempered with by decrypting the signed message digest with the sender's public key.

The X.509 format digital certificate contain the public key and an endorsement made by a Certificate Authority with its own digital signature.

6.1.3 Authentication

Use hierarchical directory to record users and network resources. Office users should be assigned accounts authenticated to use their Local Area Network via a Network operating system that is either Novell Netware or Microsoft NT. The NDS, the NDS for Windows NT or the Windows NT active directory that would come with NT5.0 may be used for individual projects.

Beyond the local area network, users should be authenticated against a common directory. This government-wide directory should be based on X.500, or comparable enterprise directory. These directories should be compatible with the Lightweight Directory Access Protocol (LDAP) and may be use to hold the certified public keys.

The public key pair for authentication should have a minimum length of 1024 bits.

6.1.4 Access control

Individual computers dial up to arbitrary Internet Service Providers (ISP) create security and performance concerns. This approach is not recommended.

6.1.4.1 Outbound Access

Outbound Internet gateway serves as a centralised point of security control and allows for deployment of common services. These outbound Internet gateways should use a template approach for implementation. Government I-Net applications for public access should be protected by an enhanced Demilitarized Zone (DMZ) configuration. The DMZ is placed between an external packet level firewall and an internal choke router. Servers for communication to the Internet are placed in the DMZ, with communication to internal servers placed inside the Internal Service Network (ISN). All network services should be disable by default and enable as per individual project requirement.

6.1.4.2 Inbound Access

Inbound Internet traffic to the ISN should not be allowed.

Inbound Internet traffic to the DMZ to support the eight application categories should be allowed. Inbound Remote Access Point (RAP) provides application access, e-mail and file transfer functions to remote government users. The use of RAP should be reviewed and rigorously controlled. Consistent with existing ITSD guidelines, remote access system implemented with caller-id and dial-back features provide better authentication over PC remote control programs.

Inbound RAP should be implemented as dial-up networking into TCP/IP or IPX network. Inbound IP log-in to any department network via an Internet gateway should not be allowed.

6.1.4.3 Internet Gateway Template

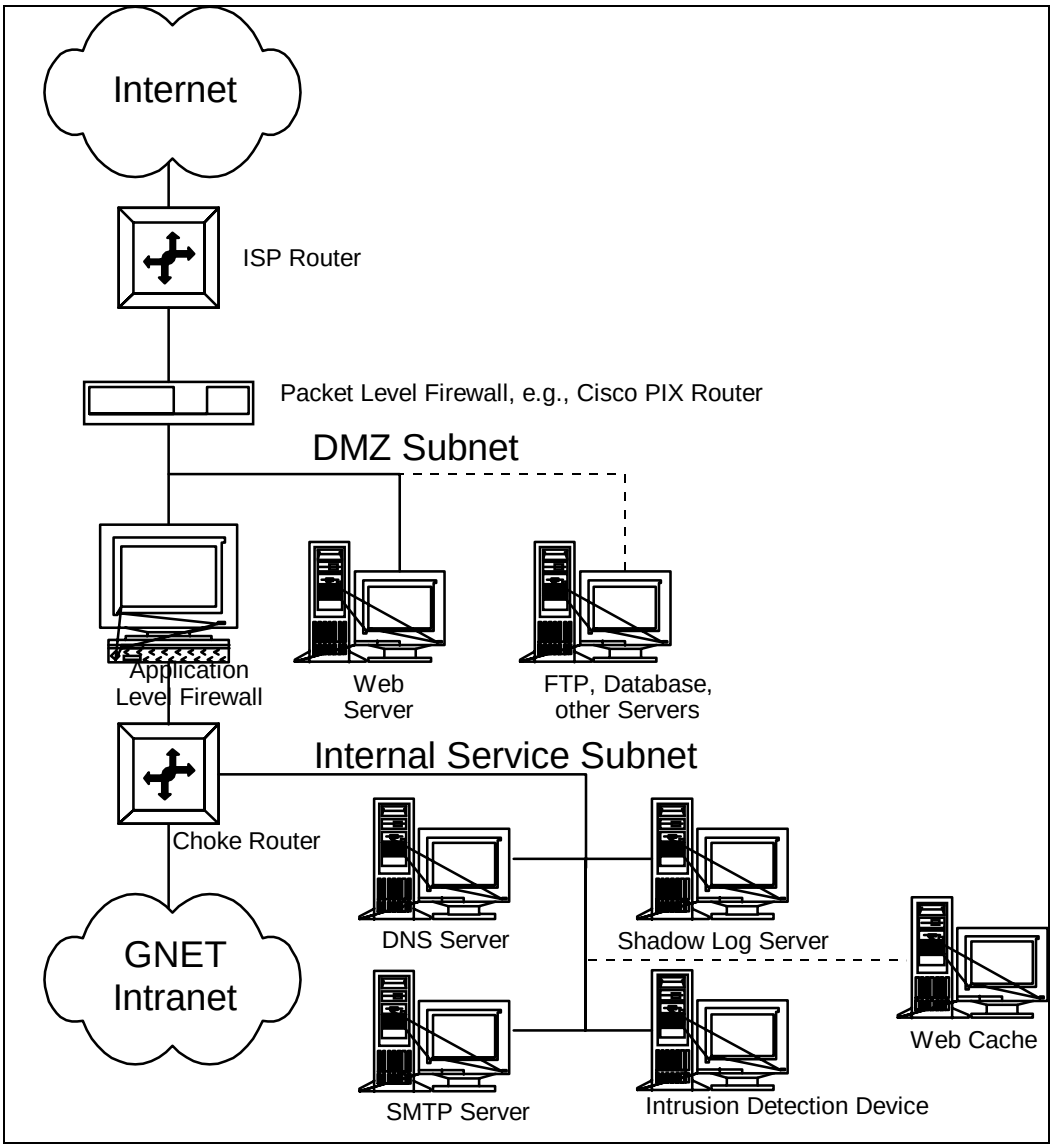


Figure 2: Internet Gateway Template

6.1.5 Availability

Availability of the Internet gateway should be enhanced by choosing UNIX machine as server hosts. Clustering of processors and consolidation of storage into enterprise storage subsystems with resilient features may further increase reliability.

6.2 INTERNET LEGAL ISSUES

6.2.1 Validity and Enforceability of contract

Normal real or implied contracts are established through practices and supported by case law. When the relationship is established over the Internet, there are neither established practices nor supporting case law. The validity and enforceability of contracts created using Internet over different legal jurisdiction area create new challenges.

Digitally signed messages can be introduced as evidence into a trial. The appropriate security procedures, documentation, and an effective audit trail should be available regarding the creation and certification of the public keys used for digital signatures.

6.2.2 Law on electronic commerce

Contracts to be executed over the Internet should comply to local law and satisfy the World Trade Organisation requirement of 'fair and open'.

6.2.2.1 The Electronic Transactions Ordinance

To provide a favourable environment for electronic business to take place in Hong Kong, there is a need to establish a clear legal framework to provide for certainty in the conduct of electronic transactions. The Electronic Transactions Ordinance (Cap. 553) was enacted by the Legislative Council on 5 January 2000 and gazetted on 7 January 2000.

The details of the Ordinance is available at the Bilingual Laws Information Systems (www.justice.gov.hk).

6.2.2.2 Recognition of Certification Authorities and Certificates

The record of recognized certification authority is maintained by the Director of Information Technology Services and available for public access on-line at www.info.gov.hk/itsd.

6.2.3 Standard Disclaimers

Government Web sites should contain standard set of disclaimers on their home pages regarding the limit to the accuracy of the information posted. The recent disclaimers appeared on the Government Information Centre (GIC) and Year 2000 Web sites are extracted at Annex A for reference. Individual Web sites should develop site-specific disclaimer according to the nature of the site and seek appropriate legal advice.

6.3 INTERNET PRIVACY ISSUES

6.3.1 Impact of Privacy Ordinance

The Personal Data (Privacy) Ordinance (PDPO) brought into force in December 1996 protects the privacy interests of individuals in relation to personal data. It gives rights to data subjects to confirm with data users whether their personal data are held in a lawful manner, to obtain a copy of such data, and to have personal data corrected.

The six Data Protection Principles of the PDPO cover the purpose and manner of collection, accuracy and duration of retention, use of personal data, security of personal data, information to be generally available, as well as access to personal data. Like other I.T. systems, I-Net applications for the HKSAR Government are subject to the requirement of the Ordinance.

A number of Guidance Materials and Codes of Practice were issued by the Privacy Commissioner's Office (PCO) to help individuals and data users to address Internet related privacy issues and should be observed.

6.3.2 Single Sign On

Single Sign On (SSO) allows general public to access government-wide service using a single authentication process, without being re-authenticated for each service. SSO requires a central directory of users that will be shared by many different Internet applications. In the absence of suitable physical token based security device to safe guard the confidentially and privacy of the personal data, SSO should not be used in the government network.

6.3.3 Use of Data Encryption by Public

Encryption is recommended as a useful tool in protecting the confidentially of personal data.

6.3.4 Privacy Policy and Personal Information Collection Statements

Government sites hosting I-Net applications shall inform their users about their policy and practices in handling personal data by a Privacy Policy Statement (PPS).

When personal data are to be collected, the sites should provide on-line notification of a Personal Information Collection (PIC) statement. The PIC should inform users how the data are to be used, to which parties the personal data may be transferred, as well as the user's rights to request and correct the data.

The guidelines on *Preparing On-line Personal Information Collection (PIC) Statements and Privacy Policy Statements (PPS)* issued by the PCO are recommended reference.

6.3.5 Use on the Identity Card Number and Other Personal Identifiers

I-Net applications should observe the *Code of Practice on the Identity Card Number and other Personal Identifiers*. Data users have no right to compel an individual to provide an ID card number unless authorised by law.

6.4 WEB CONTENT ACCESSIBILITY

Using web technology to access information is more and more common in our daily lives. As the Web community diversifies in their abilities and skills, it is crucial that information relevant to our lives is accessible by the public at large including different disability groups. For the purpose, W3C has published a recommendation *Web Content Accessibility Guidelines 1.0* in May, 1999.

In order to facilitate different disability group to access the information in the web pages, I-Net applications that require publishing information to the general public are advised to adopt appropriate accessibility features suggested in the guidelines.

7. TAIGA APPLICATION CATEGORIES

The eight TAIGA application categories were messaging; navigation; delivery; collaboration; database query and update; order, ship and bill; online payment and online purchase. Each of the eight application categories incorporates by reference the requirements of the previous one.

7.1 MESSAGING

The government messaging system provides the ability for users to locate recipients, compose messages, and have them efficiently delivered to one or more other users. Private and secure messaging from user to user across the Internet is an additional important function. E-Commerce requires in addition the ability to provide secure and reliable delivery.

7.1.1 Services

Messaging application should use client-server based messaging system. Messaging applications should deploy Simple Mail Transfer Protocol (SMTP) to route mail between mail servers and from client to server. SMTP may be extended through the use of Multipurpose Internet Mail Extensions (MIME) to attach multimedia contents.

The Post Office Protocol Version 3 (POP3) or Internet Message Access Protocol Version 4 (IMAP4) should be used to transfer messages from mail server to client computers.

Electronic message in Chinese language should be encoded in BIG5 scheme and supplemented by the HKSCS character set.

7.1.2 Security

Implementing S/MIME enhance integrity to the messaging application. S/MIME provides encryption and authentication functions. S/MIME v2 submitted to IETF is informational only and limits to encryption using 40 bits private key. As I-Net application should use private key with at least 128-bit key length, implementation based on the S/MIME v3 should be used. For sensitive data, authenticated with physical token is recommended.

Digital Certificates authenticate the public keys for communication. The digital certificate in the standard X.509 v3 should be validated by a Certificate Authority.

Each messaging implementation should have a postmaster with the responsibility for the timeliness and integrity of user directories and the general availability of the messaging application.

7.1.3 Communication

TCP/IP is used to communicate between the client and server mail system. For secure messaging applications, S/MIME should be deployed to provide end-to-end encryption

in addition to adopting transport level security using SSL.

LDAP complied, government-wide hierarchical directory should be established. The subsequent transition to full X.500 directory format shall be exploited. The hierarchical directory will reduce the effort to maintain the duplicated names found in the linear user directory structure.

7.2 INFORMATION NAVIGATION

Information navigation applications allow government users to browse through the collection of online documents either internal to the Government or out on the Internet to find information. The minimum user platform for these applications consists of a browser, an e-mail client, a news group reader, and various helpers and viewer applications.

7.2.1 Services

Client browser program should support the basic protocols including HTTP 1.1 and NNTP. The browser should contain the Java Virtual Machine (JVM) to allow Java applets for Internet applications to be built and operated on top of the browser.

Standard browser installation should include facilities for displaying Chinese text. Provision to load additional special character sets to be provided only after adequate instructions to the users.

7.2.2 Security

Internet gateway serves as a centralised point of security control and allows for deployment of common services.

The server and gateway operating system platform should be based on hardened UNIX machines for their scalability and additional access control.

Virus scanning should be installed at gateway and all desktops enabled for navigation application. An enterprise directory based on NetWare NDS log-in should be used for basic authentication.

7.2.3 Communication

Navigation application should use the TCP/IP software under Windows 95 environment. The network addresses should be dynamically assigned by DHCP servers and conformed to the IANA standard.

As specified under the section 6.1.1, Secure Sockets Layer (SSL 3.0) services provide the basis for authentication by the external site.

7.3 INFORMATION DELIVERY

Information delivery applications are electronic publishing on a Web server. A delivery application has two group of users: the users who navigate to the site and use the information; and the government users responsible for the day to day management of the content, ensuring accessibility from multiple browsers, ensuring adequate performance under a variety of load conditions, together with backup and recovery issues.

7.3.1 Publishing Frameworks

Content management systems can dynamically generate Web pages from contents stored in database against HTML templates. This streamlines the approval and publishing cycle while enhancing the reliability.

7.3.2 Services

Request from Web client to Web server should use the Hyper Text Transfer Protocol (HTTP 1.1). Web server retrieves the information previously created with Hyper Text Markup Language (HTML 4.0) and pass to the Web client. The Web client renders and displays the page for the user according to the HTML protocol. It is desirable to support the FTP protocol and portable document format for delivery of large documents.

Information delivery applications should implement topic indexes and site overviews. They should provide standard search function using keyword and Boolean operations. The content in Chinese should use the standard BIG5 encoding scheme plus support of HKSCS character set.

The applications may use established 4GL products, Java, Javascript, and Perl on the server side. The client side may be Java, Javascript, Jscript, and Visual Basic as appropriate.

The design should avoid assumption on the use of a particular brand of browser. ActiveX should only be used if it is assured that all clients are Win32 platform supporting DCOM.

7.3.3 Security

Digital signature may be implemented on the Web pages to confirm integrity of the document.

There should be a Webmaster with the responsibility for the organisation of the Web pages on the server, the contents and its presentation, monitoring and reporting on usage of the site to its sponsor and the general availability of the server.

7.3.4 Communication

As specified under the section 6.1.1, Secure Sockets Layer (SSL 3.0) service provides

the basis for authentication of the external site.

7.4 COLLABORATION

Collaboration application builds on the information delivery application to facilitate users to contribute documents and carry on discussions on a formal or informal basis. This contrasts with an information delivery application which requires a more disciplined approach to ensure the quality and timeliness of the contents.

7.4.1 Services

Network News Transfer Protocol (NNTP) is the native protocol to be supported for newsgroups. The newsgroups of the collaboration application in Chinese should use the standard BIG5 encoding scheme plus support of HKSCS character set.

7.4.2 Security

The use of UNIX machines should be considered for availability and security.

For collaboration application implemented for public access using NNTP protocol, there should be two NNTP servers. One should be hosted in the DMZ for the public and the other should be hosted in the Internal Service Network for users in all departments (6.1.4.3). The latter should contain a superset of the newsgroups on the public server.

Each collaboration implementation should have a person assumes the role of Newsmaster. The responsibility includes moderating the discussing, imposing access control of posters and readers, monitoring and reporting on usage of the site to its sponsor and the general availability of the server.

7.4.3 Communication

The collaboration servers for public access should reside on the DMZ. The security consideration for setting up public accessed servers should be observed.

7.5 DATABASE QUERY AND UPDATE

Database query and update applications (DBQ) allow users to query database, and lead them through registration and other update operations. Confidential information may be exchanged but no on-line financial transaction will be involved.

7.5.1 Services

Application development for DBQ applications should use languages already standardised on by ITSD and supplemented with Java. Established 4GL products may be used on the server. They may invoke application modules written in language like C++, Java, and Visual Basic using vendor's API.

Consistent with normal client-server applications development, interface from Web server tier to the database tier should use SQL-89 via ODBC.

The database may be located in the DMZ or replicated from existing database in the internal network onto the DMZ. For large and volatile database where replication is not be feasible, traffic on specific TCP/IP ports may be arranged through the firewall to access the database inside the internal network.

7.5.2 Security

DBQ application that updates personal information should be authenticated using digital certificates. This requires a CA to issue X.509 v3 format certificates to confirm validity of the users' public key. This may be an existing CA that could validate the user's public key against some of the users' credential. If justified, the application may establish its own CA for the particular application and issue certificate to the registered users of that application.

The UNIX or MVS systems should be considered as the host platform for DBQ applications as they are more scaleable versus Windows NT. Both UNIX and MVS may be configured as cluster server to enhance the availability.

7.5.3 Communication

The general design of I-Net applications should be multi-tiered, loosely-coupled and application messaging based. The basic DBQ applications are three-tiers that contains Web clients, Web server and database server.

Communication between Web client and Web server should use HTTP and HTML as specified in the category of information delivery.

Communication between Web server and application server should be performed by a middle layer of software called middleware. The three common types of software layer, in increasing level of complexity, are Common Gateway Interface, Object Request Brokers and Message Oriented Middleware. In the case there are multiple application server using different middleware, XML should be considered as the standard for application integration.

7.5.3.1 Common Gateway Interface (CGI)

Common Gateway Interface (CGI) is a programming interface that is called from the Web server. Access to external database using CGI is simple but involves substantial runtime overheads, this may be used for applications with low transaction volume.

7.5.3.2 Object Request Brokers (ORB)

The Object Request Brokers (ORB) is the dynamic object linking mechanism over which objects can interact with other objects located locally or remotely. ORB should be used for high transaction volume applications. The two current competing ORB protocols are Microsoft DCOM and OMG CORBA.

- Cross platform interoperability is the key advantage of CORBA over DCOM. CORBA is recommended as it provides a much smoother interface to a wide variety of existing government systems.

- DCOM should be used sparingly when the application focus is on integration with Windows 95 ActiveX enabled programs.

7.5.3.3 Message Oriented Middleware (MOM)

Middleware connects two and more computers working on the same task distributed across different tiers. Message Oriented Middleware (MOM) is event-driven and should be used for connecting computers on latency or intermittently connected networks. The use of MOM may be exploited to supplement CORBA.

7.6 ORDER, SHIP AND BILL

Order, ship and Bill (OSB) is considered as a subset of electronic commerce applications in which persons and businesses purchase things or services from the government on a mainly though not exclusively discretionary basis. The Order, Ship and Bill application category encompasses applications in which payment is needed, but for which on-line payment is not required.

7.6.1 Application Frameworks

Application frameworks from vendors compose of shared modular services, protocols, languages, development as well as run time environments. These inter-operable elements should be picked based on compatibility with IETF and the architecture elements of TAIGA.

The framework should be evaluated on cost, performance and flexibility in respect to support of standards, secure and efficient user management, as well as coexistence with existing messaging systems. It is also important to consider features include Chinese language support, content management, database integration and third party support. TAIGA allows for elements from any number of vendor application frameworks to be operational at any given time.

The major application frameworks key vendors -- in alphabetical orders -- are IBM Commerce Point, Microsoft Internet Commerce Framework (ICF), Netscape Open Network Environment (ONE), Oracle Web Applications System (WAS), and Sun Java Electronic Commerce Framework (JECF).

7.6.2 Services

Application development for OSB applications should use languages already standardised on by ITSD and supplemented with Java. Established 4GL products may be used on the server. They may invoke application modules written in language like C++, Java, and Visual Basic using vendor's API.

Consistent with normal client-server applications development, interface from Web server tier to the database tier should use SQL-89 via ODBC.

The database may be located in the DMZ or replicated from existing database in the internal network onto the DMZ. For large and volatile database where replication is not be feasible, traffic on specific TCP/IP ports may be arranged through the firewall to access the database inside the internal network.

7.6.3 Security

OSB application that updates personal information should be authenticated using digital certificates. This requires a CA to issue X.509 v3 format certificates to confirm validity of the users' public key. This may be an existing CA that could validate the user's public key against some of the users' credential. Pending the result of the study for the government-wide CA function, the application may establish its own CA for

the particular application and issue certificate relevant to the application.

As normal form posting methods from the client to the server are not encrypted, enrollment and order forms with contents that need to be secured should only connect to the server through SSL.

Each invoice or billing operation in an OSB application as well as any changes to the original request shall be stored and logged in an audit trail. This ensures that the transaction history is recoverable to its original form in the event of disputes.

The contents of the order and financial arrangement should be treated as personal data with the privacy issues in section 6.3 observed.

7.6.4 Communication

The communication services of OSB application should be the same as DBQ application category.

7.7 ONLINE PAYMENT

Online payment applications extend the OSB application and compute an order total amount and allow immediate online payment. Examples of online payment applications include purchasing postage stamps, purchasing maps, paying licensing and other fees. The main form of payment available through the Internet is credit card payment.

7.7.1 Services

Secure Electronic Transaction (SET) protocol should be used for sending encrypted credit card numbers over Internet for payment purpose. SET provides buyers and merchants with Internet transaction support managed by a trusted third party (the bank). SET provides for integrity and authentication, but not confidentiality of its data items other than the credit card number.

Major banks in Hong Kong had already announced the establishment of SET payment gateway, the actual charging rate and scheme of the gateway, as well as the liability issues of payment via credit card need to be addressed depending on the requirement of the individual project.

Government departments who plan to provide services with on-line payment is recommended to observe the development and study the impact.

7.7.2 Security

Mutual authentication is provided through digital signatures and certificates. SET protocol requires the establishment of a public CA to issue the cardholder and merchant certificates.

7.7.3 Communication

The communication services of online payment application should be the same as DBQ application category.

7.8 ONLINE PURCHASE

This category includes tendering and transaction of government purchasing. Online purchasing applications should consider the security in messaging and data storage, and interaction with legacy systems. The entire online purchasing cycle should be built as I-Net applications consolidated from several categories.

- Dissemination of tender information and documents should be built as an information delivery application.
- Receiving of tendering bids should be built as a DBQ application using encryption.
- Contract Management should be built as an DBQ application
- Delivery of procurement services should be built as OSB application.

7.8.1 Services

For supplier communication where application messaging is required, the United Nation / Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) standard framework may be used for encoding of messages.

7.8.2 Security

The purchase application should authenticate the users using multiple use passwords and digital certificates. This requires a public CA that could issue X.509 v3 format certificates to confirm validity of the public key of both parties.

Confidential information for a purchase application requires end-to-end encryption using S/MIME. Application level communication between the tender site and the government internal database may be encrypted using SSL v3.

7.8.3 Communication

The communication services of online purchase application should be the same as DBQ application category.

ANNEX A - SAMPLE DISCLAIMERS

1. Disclaimer Extracted from the Government Information Centre (GIC) Web site

" This Web site is produced and maintained by the Information Services Department, Hong Kong Special Administrative Region (HKSAR) of the People's Republic of China. The HKSAR was established on July 1, 1997.

This Web site is best viewed with Netscape or Internet Explorer 3.0 or above.

Updating in this Web site is carried out as soon as new information is available. However, there is no warranty or responsibility of any kind on providing accurate information and data at a particular point of time.

Permission is required in adopting photographs and graphics of this Web site onto other home pages. Please send your request to piopub@isd.gcn.gov.hk

Overseas Internet users should note that the telephone numbers and facsimile lines of Hong Kong are preceded by the area code "852". Updating in this Web site is carried out as soon as new information is available. However, there is no warranty or responsibility of any kind on providing accurate information and data at a particular point of time. "

(URL http://www.info.gov.hk/absite.htm)

2. Disclaimer Extracted from the Government Year 2000 Web site

" All the guidelines, documents and software in this directory are primarily prepared for use by the Hong Kong Special Administrative Region (HKSAR) Government Departments at their specific hardware/software environment. The information published in this directory is offered for information only and provided "AS IS". The HKSAR Government makes no warranty, express or implied, as to the accuracy or completeness of any information in the guidelines, documents and software.

The HKSAR Government does not warrant or guarantee, either explicitly or implicitly, that the products of the vendor community will conform to the information provided in this directory. Any reference or references within the guidelines, documents and software in this directory to any specific commercial product, service or firm, by trade name, trade mark, manufacturer or otherwise, does not constitute or imply any endorsement or recommendation by HKSAR Government.

The HKSAR Government makes no express or implied warranties of merchantability or fitness for a particular purpose or use with respect to any information, data or software whatsoever in this directory. Under no circumstances will HKSAR Government be held liable to any third party who may choose to rely on the information, data or software in this directory for planning or other purposes. "

(URL http://www.year2000.gov.hk/info/disclaimer.htm)