

STATE SERVICES COMMISSION  
Te Kōmihana O Ngā Tari Kāwanatanga



**New Zealand E-government  
Interoperability Framework  
(NZ e-GIF)**

**Version 3.1**

**INTRODUCTION**

**November 2006**

State Services Commission

Te Kōmihana O Ngā Tari Kāwanatanga

## **Foreword**

The E-government Interoperability Framework (e-GIF) was first issued in February 2002. This version (v3.1) is the eighth edition to be published.

In the three and a half years since the initial launch, we have seen tremendous change in New Zealand, both in the public sector and in wider society. Technology continues to advance and government agencies' business needs keep evolving in response to the changes in technology and society. The challenges and opportunities these changes present demand innovative and collaborative solutions from government agencies.

Since 2002, the e-GIF has proved to be a significant tool for enabling agencies to work together and for all-of-government initiatives. By promoting collaboration and the efficient use of resources, the e-GIF contributes to the State Services Development Goals of Networked, Coordinated and Accessible State Services.

The e-GIF has formed the foundation of a number of important e-government initiatives. The framework has helped collaboration between government agencies, resulting in more integrated services for New Zealanders. For example:

- Customers can now register for a company IRD number online when they incorporate a company. This service eliminates the need for new companies to deal with the Companies Office and Inland Revenue separately. It makes the registration process faster by eliminating duplication of information between agencies and the need to provide paper-based IRD number applications.
- SEEMail, the Secure Electronic Environment Mail standard, helps the secure exchange of email and attachments using the Internet. It is now used by 51 government agencies.
- [www.govt.nz](http://www.govt.nz), the all-of-government web portal, uses e-GIF standards to collect information about government services from a wide range of government agencies. It provides an online single point of access for New Zealanders.

These online services and resources have been made possible by the e-GIF, and the people from across government who have worked together on this version, and all the earlier versions, of the framework.

Over the coming years standards will continue to be added to the e-GIF, and the framework will grow to accommodate them.

We welcome the publication of this latest version and acknowledge the collaborative effort that has achieved this. We are also confident this valuable resource will continue to provide the foundation for future e-government initiatives across the State Services.

Laurence Millar

Deputy Commissioner, Information and Communication Technologies Branch

Warren Tucker

Chairperson, e-GIF Management Committee

## **About the e-GIF documents**

The E-government Interoperability Framework (e-GIF) Version 3.1, consists of three documents:

- Part 1: Standards
- Part 2: Policy
- Part 3: Resources

Below are short descriptions of each document and its intended audience.

### **Part 1: Standards**

Part 1 focuses on the standards that make up the e-GIF. The intended audience for this section includes:

- State sector information technology (IT) strategists
- technical analysts
- programme and project managers
- anyone planning services requiring interoperability.

Part 1 includes the following sections:

- **How to read the standards:** Description of the layer model used to categorise the standards, what the status levels for each standard mean, links to related documentation, and changes from the last e-GIF.
- **e-GIF standards:** The standards listed by category.
- **E-government services:** Services that are part of the e-government programme, fully support interoperability, and are freely available to public sector agencies.

### **Part 2: Policy**

Part 2 outlines the policy behind the e-GIF and its development. The intended audience for this section includes:

- policy analysts
- advisors
- business analysts
- anyone involved with interoperability strategy and projects.

Part 2 includes the following sections:

- **What is the e-GIF?** Short descriptions of e-government, interoperability, and the e-GIF, how the e-GIF will benefit New Zealand, and how the e-GIF is maintained.
- **Who must comply and when?** Who must comply with the e-GIF, how to transition to e-GIF compliance, exemptions and special provisions.
- **Principles:** Short descriptions of anticipated outcomes of the e-GIF, requirements for project and operational management, and governance principles.
- **Developing the e-GIF:** Outlines of procedures for extending the e-GIF, submitting a new standard, developing the framework, and issues under review or proposed for future working groups.

### **Part 3: Resources**

Part 3 contains resources related to the e-GIF. The intended audience for this section is all readers of the e-GIF.

Part 3 includes the following sections:

- **History of the e-GIF:** Review of stages in the e-GIF's development, including a Change Log.
- **References and background information:** Descriptions and links to further information related to the e-GIF.
- **URLs referred to in the e-GIF:** Full URLs for all hyperlinks in the e-GIF documents.
- **Abbreviations:** Definitions of abbreviations and acronyms used in the e-GIF.

STATE SERVICES COMMISSION  
Te Kōmihana O Ngā Tari Kāwanatanga



**New Zealand E-government  
Interoperability Framework  
(NZ e-GIF)**

**Version 3.1**

**PART 1 – STANDARDS**

**November 2006**

State Services Commission

Te Kōmihana O Ngā Tari Kāwanatanga

## **About this document**

This document focuses on the standards that make up the e-GIF. The intended audience for this Standards section includes:

- State sector information technology (IT) strategists
- technical analysts
- programme and project managers
- anyone planning services requiring interoperability.

It includes the following sections:

- [How to read the standards](#): Description of the layer model used to categorise the standards, what the status levels for each standard mean, links to related documentation, and changes from the last e-GIF.
- [E-GIF standards](#): The standards listed by category.
- [E-government services](#): Services that are part of the e-government programme, fully support interoperability, and are freely available to public sector agencies.

## Table of Contents

<b>New Zealand E-government</b> .....	<b>i</b>
<b>Interoperability Framework</b> .....	<b>i</b>
<b>(NZ e-GIF)</b> .....	<b>i</b>
<b>Version 3.1</b> .....	<b>i</b>
<b>PART 1 – STANDARDS</b> .....	<b>i</b>
<b>November 2006</b> .....	<b>i</b>
<b>1 How to read the standards</b> .....	<b>1</b>
<b>1.1 Layer model</b> .....	<b>1</b>
<b>1.2 Compliance status levels</b> .....	<b>4</b>
<b>1.3 Current e-GIF compliance status levels</b> .....	<b>5</b>
<b>1.4 Choosing between standards</b> .....	<b>7</b>
<b>1.5 Links</b> .....	<b>7</b>
<b>1.6 Comments</b> .....	<b>8</b>
<b>1.7 Changes from previous version</b> .....	<b>8</b>
<b>2 e-GIF standards</b> .....	<b>9</b>
<b>2.1 Network layer</b> .....	<b>9</b>
2.1.1 Network protocols .....	9
2.1.2 Directory protocols .....	9
2.1.3 File transfer protocols.....	9
2.1.4 Mail transfer protocols.....	10
2.1.5 Registry services.....	10
2.1.6 Time protocols .....	11
2.1.7 Messaging transport.....	11
2.1.8 Messaging formats.....	11
<b>2.2 Data Integration layer</b> .....	<b>12</b>
2.2.1 Primary character set.....	12



2.2.2	Structured web document language .....	12
2.2.3	Schema definition languages .....	12
2.2.4	Document type definition .....	12
2.2.5	Structured data .....	12
2.2.6	Batch/bulk data.....	13
2.2.7	File compression .....	13
2.2.8	File archiving .....	13
<b>2.3</b>	<b>Business Services layer.....</b>	<b>14</b>
2.3.1	Metadata (Discovery) .....	14
2.3.2	Namespace .....	14
2.3.3	Schemas .....	15
2.3.4	Structured data description.....	15
2.3.5	Name and address .....	15
2.3.6	Additional customer information .....	15
2.3.7	Customer relationship.....	16
2.3.8	E-learning .....	16
2.3.9	Business reporting.....	16
2.3.10	Directory services.....	16
2.3.11	Statistical data and metadata .....	16
2.3.12	Geospatial .....	17
2.3.13	Registry services .....	17
2.3.14	Content syndication and channel feeds.....	17
2.3.15	Instant messaging .....	18
2.3.16	Voice Over Internet Protocol (VOIP).....	18
2.3.17	Digitisation .....	19
<b>2.4</b>	<b>Access and Presentation layer.....</b>	<b>20</b>
2.4.1	Website presentation.....	20
2.4.2	Web design and maintenance .....	20
2.4.3	Forms .....	20
2.4.4	Authentication standards .....	20
<b>2.5</b>	<b>Web Services layer .....</b>	<b>22</b>
2.5.1	Discovery.....	22
2.5.2	Description .....	22
2.5.3	Access.....	22
2.5.4	Messaging .....	23
2.5.5	Security .....	23
2.5.6	Compliance .....	24
<b>2.6</b>	<b>Security layer .....</b>	<b>24</b>
2.6.1	Policy.....	25
2.6.2	Network .....	26
2.6.3	Data integration .....	27
2.6.4	Web services.....	27
2.6.5	Business services.....	27
2.6.6	Public Key Infrastructure (PKI) .....	28

<b>2.7 Best Practice layer .....</b>	<b>29</b>
2.7.1 Digital Rights Management (DRM).....	29
2.7.2 Trusted computing .....	29
2.7.3 Process .....	29
2.7.4 XML data transformation.....	30
2.7.5 Data modelling .....	30
2.7.6 Processing structured data .....	30
2.7.7 Controlled Vocabulary or code Lists (CVLs) .....	31
2.7.8 Health sector .....	31
2.7.9 Document file format.....	31
2.7.10 Biometrics .....	32
2.7.11 Evidence collection .....	32
2.7.12 Business Transactions .....	32
<b>3 E-government Services .....</b>	<b>33</b>



## 1 How to read the standards

The e-GIF standards<sup>1</sup> are categorised using a “layer model”.

Each protocol, standard or convention (de facto standard) is listed with a version number, where applicable, a status level and any relevant comments. Note that in computing, protocols are generally used to define real-time communications behaviour, while standards are used to govern the structure of information committed to long-term storage.

This section explains how to read the list of standards.

### 1.1 Layer model

Layer models are widely used to classify functions within IT systems. They are used to simplify systems by segregating system functions into levels and disentangling the complexity and variations of each level. Components normally communicate only with others at neighbouring levels, and in standardised ways.

The model for this version of the e-GIF is illustrated and described below.

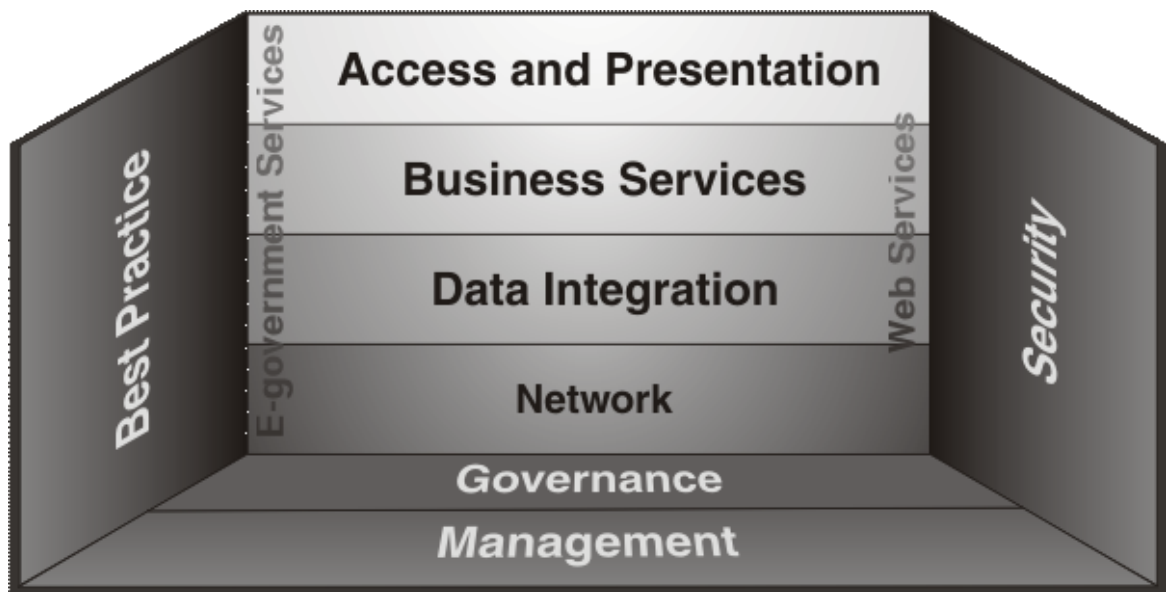


Figure 1: e-GIF v3 Layer Model

---

<sup>1</sup> In the e-GIF, protocols and standards are both referred to as “standards”. Note that protocols are sometimes distinguished as a specific type of standard — see [http://en.wikipedia.org/wiki/Protocol\\_%28computing%29](http://en.wikipedia.org/wiki/Protocol_%28computing%29) and [http://en.wikipedia.org/wiki/Communications\\_protocol](http://en.wikipedia.org/wiki/Communications_protocol).

The four basic structural components, or layers, of this model are:

- **Network:** Covers details of data transport, such as network protocols. This is a crucial area for interoperability. Without agreement on networking standards, it is hard or impossible to make systems communicate. The e-GIF uses a subset of the widely proven Internet Protocol suite.
- **Data Integration:** Facilitates interoperable data exchange and processing. Its standards allow data exchange between disparate systems and data analysis on receiving systems.
- **Business Services:** Supports data exchange in particular business applications and information contexts. Some of the standards in this layer are generic, covering multiple business-information contexts. Others work with data integration standards to define the meaning of the data, mapping it to usable business information. For example, an agency will format a stream of name-and-address data in XML (Data Integration) using the business rules of xNAL (Business Services) to create a commonly agreed representation of name-and-address information.
- **Access and Presentation:** Covers how users access and present business systems. Most of the standards in this layer are in the [Government Web Standards and Recommendations](#).

Applying to all of the structural layers are:

- **Security:** Crosses all layers, to reflect the fact that security needs to be designed into a system, not added as a layer on top. The e-GIF contains standards at the various levels designed to offer different levels of security as appropriate. It also refers to a series of standards and policy statements (the NZSITs), which provide advice and direction on the levels required.
- **Best Practice:** This is a new category to help readers of the e-GIF distinguish published standards from Best Practice, Codes of Practice, and other general or sector-focussed guidance. Published standards alone do not ensure interoperability. They merely offer a common approach to managing and understanding the context of the information exchange.
- **E-government Services:** These are actual implementations of IT infrastructure, which the ICT Branch of the State Services Commission makes available for public sector agencies to use. (See Section 3

E-government Services).

- **Web Services:** Web Services connect services together. They are an emerging set of standardised applications to connect and integrate web-based applications over the Internet. Using Best Practice implementations, agencies can agree a common approach to interoperable service delivery to customers.

Underpinning all these layers are:

- **Management:** See Part 2, Section 1.4 [Managing the e-GIF](#).
- **Governance:** See Part 2, Section 1.4 [Managing the e-GIF](#) and Section 3.4 [Governance Principles](#). An e-GIF Governance Overview paper is also available from the ICT Branch of the State Services Commission. Please email [e-GIF@ssc.govt.nz](mailto:e-GIF@ssc.govt.nz).

## **1.2 Compliance status levels**

The status level of an e-GIF standard shows its maturity relative to other standards. In 2004, the e-GIF Management Committee agreed revised status levels for e-GIF standards. The Committee renamed Mandatory and Recommended levels and extended them to include the following levels: **Adopted**, **Recommended**, **Under Development**, and **Future Consideration**. The revised status levels broadly align with those used in the UK e-GIF<sup>2</sup>. The requirement for an additional category, **Deprecated**, became evident in 2005.

The e-GIF does not require a standard to pass through each successive stage of development. When the Committee publishes an e-GIF standard, it gives it an appropriate status. When the standard matures, the Committee can consider recommendations to change its status.

---

<sup>2</sup> The criteria for status levels have been adapted from the UK e-GIF Interoperability Working Group draft paper “Criteria for TSC standards V1.doc”.

### 1.3 Current e-GIF compliance status levels

The current e-GIF compliance status levels for standards are illustrated and described below.

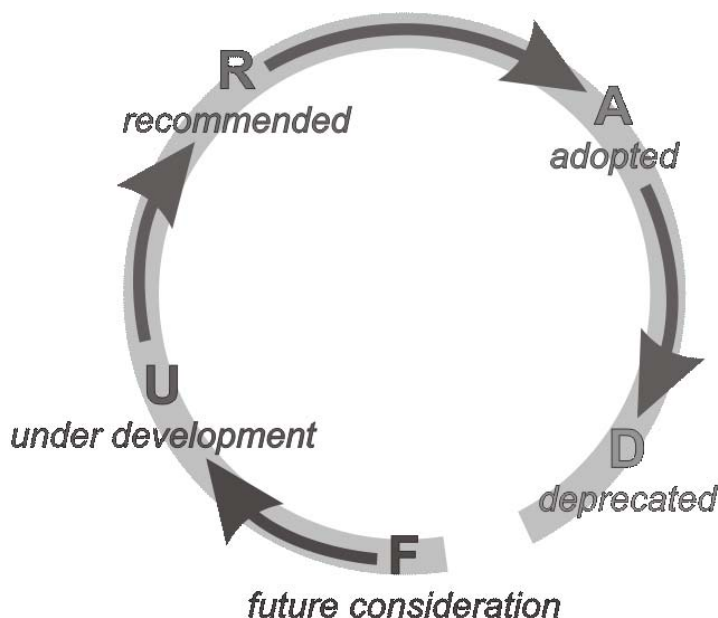


Figure 2: e-GIF Compliance Status Levels

The compliance status levels in this version of the e-GIF are:

- **Future Consideration (F):** Not yet reviewed, customised, or having any successful, documented implementation in the New Zealand government; yet probably necessary for public sector IT systems. Included mainly to introduce these standards to IT developers. F-level standards are:
  - possibly required for interoperability of IT systems in the public sector
  - open or demonstrating the intention of being open once published
  - not overruled by an existing international standard
  - not clashing with or rival to a standard already listed.
- **Under Development (U):** Actively under assessment by more than one government agency, e.g. having an active working group, a proof of concept, or a pilot implementation with associated documentation. Active or starting within three months of publication. U-level standards are:
  - required for interoperability of IT systems in the public sector
  - open or demonstrating the intention of being open once published
  - not overruled by an existing international standard



**e-GIF Version 3.1**  
**PART 1 - STANDARDS**

- not clashing with or rival to a standard already listed
- published or very soon to be published.
- **Recommended (R):** Emerging from the development, review, or Working Group process with implementation documentation and evidence of successful interoperability and data exchange. Recommended standards are generally more recent, founded upon newer technologies or standards. R-level standards are:
  - open
  - scalable
  - not overruled by an existing international standard
  - not clashing with or rival to a standard already listed
  - complete and published
  - showing clear indication of market support
  - likely to be required for interoperability of IT systems in the public sector.
- **Adopted (A):** Mandatory and normally upgraded from Recommended status (only in exceptional circumstances can a standard enter the e-GIF as Adopted without first completing a successful period as Recommended). A-level standards are:
  - required for interoperability of IT systems in the public sector
  - meeting or surpassing all criteria from the previous status levels
  - well established in public sector ICT systems
  - having complete supporting documentation and processes for implementation
  - proven effective for interoperability.

**Note:** The main difference between Recommended and Adopted is the maturity, which can be equated with well-understood software version models.

- A standard that is Adopted has widespread use and industry acceptance. It is the default standard in use, and is not expected to become Deprecated within 12 months. There is no immediate onus on existing interoperability agreements to migrate to the newer Recommended standard.

- Where a standard is Recommended, there is growing industry adoption. New interoperability initiatives are more likely to use this standard.
- **Deprecated (D):** A standard or practice that has been abandoned for, or superseded by, a better solution at the Adopted or Recommended levels. Agencies should plan to migrate away from solutions with this designation as soon as practical. New use of this standard is discouraged.

#### **1.4 Choosing between standards**

Given the need to maintain the e-GIF so that it keeps pace with changing technology, multiple standards may be available for a particular application. Agencies collaborating on interoperability projects may need to either agree one standard or use mapping technologies to achieve interoperability.

When choosing a standard:

- first consult agencies whose functions and services relate to your own (your likely interoperability partners)
- then, together, agree a standard, considering the compliant status levels:
  - Use **Recommended (R)** standards if you can; they are generally newer and less subject to obsolescence than other standards.
  - If you cannot use **R**, then use an **Adopted (A)** standard. An **A** standard is the default; but an **R** standard is preferable if it exists.
  - If you cannot use **R** or **A** standards, use any applicable **Future Consideration (F)** or **Under Development (U)** standards. Notify the ICT Branch of the State Services Commission for Working Group information and to document your implementation as part of the standards development process.
  - If no current standards apply, or you wish to propose a new standard, first please contact the ICT Branch for Working Group information.
  - Avoid new use of **Deprecated (D)** standards.

Note there may be circumstances where agencies agree to use a more mature standard (e.g. **A**) over one that is likely to have a longer life cycle (e.g. **R**). They may also accept the risk of a newer standard (e.g. **F** or **U**) instead, with the understanding that they will be taking part in its development.

#### **1.5 Links**

Standards included in the e-GIF that are [blue and underlined](#) have links to an RFC or other resources on the Internet, which explain them more fully. If you are

using a hard copy version of this document, see Part 3, Section 2 [URLs referred to in the e-GIF](#).

## **1.6 Comments**

The comments in the list of standards provide additional information on the background, circumstances of use, or anecdotal feedback that may help agencies in their decision to use or implement the applicable standard.

## **1.7 Changes from previous version**

This version of the e-GIF contains only minor editions and corrections, as well as updated references where more recent versions of referenced documents have become available. The following changes have been made:

- **Authentication section:** Section 2.4.4 added Security Assertion Messaging Standard (NZSAMS)
- **Business Services section:** Section 2.3.17 added Digitisation standard
- **Best Practice section:** Section 2.7.9, removed reference to Parliamentary Counsel Office in Open Document standard, as this reference was no longer valid.

The following elements in the list of standards were new to e-GIF v3.0:

- **Status levels:** Version 2.1 standards were either Mandatory or Recommended; this version uses the scheme described in [Section 1.3](#).
- **Standards listing:** The list of standards now notes the status level of each standard and includes relevant comments.
- **Web Services section:** [Section 2.6.4](#) includes standards specifically related to web services implementation that do not strictly fit into the layer model.
- **Best Practice section:** [Section 2.7](#) includes standards that do not strictly fit into the layer model but rather apply only in a particular context.
- **Added, moved, removed, revised standards:** See Part 3, Section 1.4 [Change Log](#). Note there are a number of new standards in the e-GIF v3.0; many of these were considered necessary to implement existing e-GIF standards.

## 2 e-GIF standards

This section sets out the current and emerging standards required for e-GIF compliance and to facilitate interoperability.

- See **Part 3, Section 3 Abbreviations** for [definitions of abbreviations](#) and acronyms used in this section.
- See **Part 3, Section 1.4 Change Log** for a [list of standards that are new, moved, removed, or changed in this version](#).
- **Links** in the list of standards to online resources, usually the standards themselves, explain more fully what each standard covers; see also [Part 3, Section 2](#) URLs referred to in the e-GIF.
- Note that **multiple standards** may exist in any category; see Section 1.4 Choosing between standards.

### 2.1 Network layer

This section covers details of data transport, such as network protocols, which is a crucial area for interoperability. Without agreement on networking standards it is hard or impossible to make systems communicate. The e-GIF uses a subset of the widely proven Internet Protocol suite.

#### 2.1.1 Network protocols

<a href="#">IP v4</a>	<b>Internet Protocol Version 4</b>
<b>Status</b>	Adopted
<b>Comments</b>	Plan for migration to IP v6. New hardware should support IP v4 as well as IP v6.

<a href="#">IP v6</a>	<b>Internet Protocol Version 6</b>
<b>Status</b>	Recommended
<b>Comments</b>	When implementing IP v6, configure routers to “ghost” IP v4.

#### 2.1.2 Directory protocols

<a href="#">LDAP v3</a>	<b>Lightweight Directory Access Protocol Version 3</b>
<b>Status</b>	Recommended
<b>Comments</b>	For access to directory services.

#### 2.1.3 File transfer protocols

<a href="#">FTP</a>	<b>File Transfer Protocol</b>
<b>Status</b>	Adopted for file transfers, where security is not required.

### **Secure File Transfer Protocols**

Please note that secure file transfer protocols (such as Secure Copy and SSH File Transfer Protocol) are under review. Agencies considering products are advised to contact the [ICT Branch](#).

**Comments** Use restart and recovery. Also [FTP security extensions](#) and [FTP via Port 80](#) where applicable.

### **[HTTP v1.1](#) HyperText Transfer Protocol Version 1.1**

**Status** Adopted

**Comments** Application level protocol. See [Security layer](#) for secure HTTP (HTTPS) and TLS usage.

### **[WebDAV](#) World Wide Web Distributed Authoring and Versioning**

**Status** Future Consideration

**Comments** A set of extensions to [HTTP v1.1](#) that allows users to collaboratively edit and manage files remotely but avoids access problems with NAT firewalls.

### **[SCP](#) Session Control Protocol**

**Status** Future Consideration

**Comments** SCP is a simple protocol, which lets a server and client have multiple conversations over a single TCP connection. The protocol is designed to be simple to implement, and is modelled after TCP.

## **2.1.4 Mail transfer protocols**

### **[SMTP](#) Simple Mail Transfer Protocol**

**Status** Adopted

**Comments** Host-to-host protocol. Beware of [spoofing](#) of email addresses. SMTP-TLS is used to protect mail headers.

## **2.1.5 Registry services**

### **[DNS](#) Domain Name Server**

**Status** Adopted

**Comments** Use DNS for Internet/Intranet domain to IP address resolution. [DNS Security](#) is critical.

### **[LDAP v3](#) Lightweight Directory Access Protocol Version 3**

**Status** Future Consideration

**Comments** Increasingly used for internal user authentication, and certificate registries. Not recommended for cross-domain purposes.

#### 2.1.6 Time protocols

**NTP v4**      **Network Time Protocol Version 4**  
**Status**      Under Development  
**Comments**    De facto standard proposed for use in an all-of-government time standard. Best practice guidelines are available.

**UTC (MSL)**    **Universal Time Clock (Measurement Standards Laboratory)**  
**Status**      Future Consideration  
**Comments**    De facto standard (accessed from Industrial Research Limited, MSL); proposed for use in an all-of-government time standard. Best practice guidelines are available.

#### 2.1.7 Messaging transport

**HTTP v1.1**    **HyperText Transfer Protocol Version 1.1**  
**Status**      Adopted  
**Comments**    See [File transfer](#) and [Security layer](#).

#### 2.1.8 Messaging formats

**MIME**      **Multi-Purpose Internet Mail Extension**  
**Status**      Adopted  
**Comments**    See also [S/MIME](#) and [Security layer](#) for secure mail attachments. Do not use Transport Neutral Encapsulation Formats (TNEF) for headers.

## 2.2 *Data Integration layer*

The Data Integration layer outlines standards in the realm of data exchange and processes.

### 2.2.1 Primary character set

**ASCII**      **American Standard Code for Information Interchange**  
**Status**      Adopted  
**Comments**    Minimum set of characters for data interchange.

**ISO**            **8859-1**  
**Status**        Deprecated

**UTF-8**        **UCS Transformation Format (8-bit encoding)**  
**Status**        Adopted  
**Comments**    UTF-8 is a variable length character encoding for Unicode. It can represent any character in the Unicode character set, yet is backwards compatible with ASCII.

### 2.2.2 Structured web document language

**HTML v4.01** **HyperText Markup Language Version 4.01**  
**Status**        Adopted  
**Comments**    For web content. See [Web Standards and Recommendations v1.0](#).

### 2.2.3 Schema definition languages

**XML v1.0**      **Extensible Markup Language Version 1.0**  
**Status**        Adopted  
**Comments**    Meta-language to create tags to define, transit, validate, and interpret data.

### 2.2.4 Document type definition

**DTD**            **Document Type Definition**  
**Status**        Adopted  
**Comments**    Describes multiple elements and attributes for XML; see [W3School's DTD Tutorial](#).

### 2.2.5 Structured data

**XML v1.0**      **Extensible Markup Language Version 1.0**  
**Status**        Adopted

**Comments** Preferred option for structured data transport.

#### 2.2.6 Batch/bulk data

**XML** Extensible Markup Language Version

**Status** Adopted

**Comments** XML 1.0 is preferred for structured data transport. Parties must agree file header records before exchange.

**CSV** Comma-Separated Values

**Status** Deprecated

**Comments** Certain implementations of XML may fail in bulk/batch mode; in which case agencies may use deprecated standard of CSV. Parties must agree file header records before exchange.

#### 2.2.7 File compression

**ZIP v2.3** ZIP Version 2.3

**Status** Adopted

**Comments** Other products using the compression algorithm LZH are also acceptable, subject to the agreement of the exchanging parties.

**GZIP** GNU Zip

**Status** Adopted

**Comments** Not compatible with ZIP.

#### 2.2.8 File archiving

**TAR** Tape Archiver

**Status** Adopted

**Comments**



## 2.3 Business Services layer

Business Services describe the services and data from a business point of view, i.e. mapping the technical components to useful business information.

### 2.3.1 Metadata (Discovery)

[NZGLS v2.0](#) **New Zealand Government Locator Service Version 2.0**

**Status** Adopted

[NZGLS Thesauri](#) **New Zealand Government Locator Service Thesauri**

**Status** Adopted

[RDF](#) **Resource Description Framework**

**Status** Adopted

**Comments** An XML file format to describe metadata. RDF is used by RSS1.0 (see below).

### 2.3.2 Namespace

[W3C schema definitions](#) **World Wide Web Consortium Schema**

**Definitions**

**Status** Adopted

**Comments** Use when other schemas customised for use by government agencies are not specifically identified (e.g. NZGMS, xNAL (nz), NZGLS).

[OIDS](#) **Schema Object Identifiers**

**Status** Recommended

**Comments** The ICT Branch of the State Services Commission maintains 2.16.544.101 as the Government OID Arc.

[URN](#) **Uniform Resource Name**

**Status** Under Development

**Comments** A way of unambiguously defining each element type and attribute name in an XML document. Working Group led by ICT Branch of the State Services Commission. See also [RFC 4350](#).

### 2.3.3 Schemas

#### [W3C schema definitions](#) World Wide Web Consortium Schema Definitions

**Status** Adopted

**Comments** Use when other schemas customised for use by government agencies are not specifically identified (e.g. NZGMS, xNAL (nz), NZGLS).

### 2.3.4 Structured data description

#### [XML v1.1](#) Extensible Markup Language Version 1.1

**Status** Adopted

**Comments** Note: “Structured data” refers to XML Schema v1.0.

### 2.3.5 Name and address

#### [xNAL v2](#) Extensible Name and Address Language Version 2

**Status** Adopted

**Comments** xNAL (OASIS) v3 being drafted; will be incorporated into e-GIF following a successful pilot.

Note: In 2006, NZ Post issued new requirements for addressing bulk mail.

#### [xNAL \(nz\) schema](#) Extensible Name and Address Language (New Zealand)

**Status** Recommended

**Comments** Agency User Group led by ICT Branch of the State Services Commission; xNAL (nz) will ultimately be replaced by xNAL (OASIS) v3.

### 2.3.6 Additional customer information

#### [Data formats for identity records standard](#)

**Status** Under Development

**Comments** The All-of-government Authentication project used schema fragments from xCIL to develop the Identity Records standard. This specifies data formats for a range of customer-information data elements that government agencies may use in customer identity records.

#### [xCIL](#) Extensible Customer Information Language

**Status** Future Consideration

**Comments** The superset of xNAL specifying formats for customer information elements such as phone and fax number, email address, date of

birth, gender, etc. xCIL is already under consideration by several agencies and is being piloted in the web-based Change-of-Address Notification project.

### 2.3.7 Customer relationship

**xCRL**      **Extensible Customer Relationships Language**  
**Status**      Deprecated  
**Comments**      Part of the xCIL and xNAL family of standards specifying formats for relationships between customers.

**CIQ**      **Customer Information Quality**  
**Status**      Future Consideration  
**Comments**      XML Specifications for defining and managing Customer (also called "Party") information/profile (including customer/party relationships).

### 2.3.8 E-learning

**ADL, SCORM, and IMS**      **Advanced Distributed Learning, Shareable Content Object Reference Model, and Instructional Management System**  
**Status**      Future Consideration  
**Comments**      Now under the auspices of the Education Sector ICT Connectivity sub-committee.

### 2.3.9 Business reporting

**xBRL**      **Extensible Business Reporting Language**  
**Status**      Under Development  
**Comments**      Working Group underway, led by Inland Revenue.

### 2.3.10 Directory services

**DSML**      **Directory Services Markup Language**  
**Status**      Future Consideration

### 2.3.11 Statistical data and metadata

**SDMX**      **Statistical Data and Metadata Exchange**  
**Status**      Future Consideration  
**Comments**      Statistics New Zealand leads this standard.

### 2.3.12 Geospatial

**GML**      **Geography Markup Language**

**Status**      Adopted

**Comments**      Land Information New Zealand leads this standard.

**WFS**      **Web Feature Server**

**Status**      Adopted

**Comments**      Land Information New Zealand leads this standard.

**WMS**      **Web Map Server**

**Status**      Adopted

**Comments**      Land Information New Zealand leads this standard.

**ESA**      **Emergency Services in Government Administration**

**Status**      Recommended

**Comments**      Land Information New Zealand leads this standard.

**NZGMS**      **New Zealand Geospatial Metadata Standard**

**Status**      Recommended

**Comments**      Schema for identifying geospatial metadata. Land Information New Zealand leads this standard.

### 2.3.13 Registry services

**ebXML RIM and RS v2.1**      **E-business Extensible Markup Language, Registry Information Model, and Registry Services Version 2.1**

**Status**      Adopted

**Comments**      Open standard application for Registry Information and Records Services in an e-business context, as an alternative to Web Services.

**ebXML RIM and RS v3.0**      **E-business Extensible Markup Language, Registry Information Model, and Registry Services Version 3.0**

**Status**      Future Consideration

**Comments**      Open standard application for Registry Information and Records Services in an e-business context, as an alternative to Web Services.

### 2.3.14 Content syndication and channel feeds

**RSS 1.0**      **RDF Site Summary**

**Status**      Recommended

**Comments**      Note that this standard is required for agencies using the [government portal news service](#), [E-government Shared Services](#).

**RSS 2.0**      **Really Simple Syndication**  
**Status**      Future Consideration  
**Comments**    An alternative to RSS 1.0 that also enjoys wide support from the community.

**2.3.15      Instant messaging**

**XMPP**      **Extensible Messaging and Presence Protocol**  
**Status**      Future Consideration  
**Comments**    XML protocol for real-time messaging. Taken from [UK Technical Standards Catalogue Version 6.2](#).

**2.3.16      Voice Over Internet Protocol (VOIP)**

**SIP**      **Session Initiation Protocol**  
**Status**      Future Consideration  
**Comments**    A protocol for initiating, modifying, and terminating an interactive user session that involves multimedia elements such as video, voice and instant messaging. Has greater take-up than H.323. Taken from [UK Technical Standards Catalogue Version 6.2](#). [Codec](#) required.

**RTP**      **Real-time Transport Protocol**  
**Status**      Future Consideration  
**Comments**    Defines a standardised packet format for delivering audio and video over the Internet and is frequently used in conjunction with RTSP, H.323 or SIP.

**H.323 v2**    **H.323 Version 2**  
**Status**      Future Consideration  
**Comments**    An umbrella recommendation from the ITU-T, which defines the protocols to provide audiovisual communication sessions on any packet network. Taken from [UK Technical Standards Catalogue Version 6.2](#). [Codec](#) required.

**G.711**  
**Status**      Future Consideration  
**Comments**    An ITU-T standard for audio companding; primarily used in telephony.

**G.729**  
**Status**      Future Consideration

**Comments** An audio codec for voice that compresses voice audio in chunks of 10 milliseconds; is mostly used in VOIP applications for its low bandwidth requirement.

### 2.3.17 Digitisation

#### Archives Digitisation Standard

**Status** Under Development

**Comments** Archives New Zealand standard. Sets out the requirements for digitisation and disposal of paper or other analogue original source documents, and outlines best practice recommendations for digitisation processes.

## **2.4 Access and Presentation layer**

This section presents standards and guidelines covering how business systems are presented and accessed by users.

### **2.4.1 Website presentation**

#### **[New Zealand Government Web Standards and Recommendations v1.0](#)**

**Status** Adopted  
**Comments** See Web Standards and Recommendations v1.0 for use of: HTML 4.01, XHTML, GIF 89a, JPG, PNG, SVG, and PDF.

### **2.4.2 Web design and maintenance**

#### **[New Zealand Government Web Standards and Recommendations v1.0](#)**

**Status** Adopted  
**Comments** See Web Standards and Recommendations v1.0 for use of: HTML 4.01, XHTML, GIF 89a, JPG, PNG, SVG, and PDF.

### **2.4.3 Forms**

Agencies considering products are advised to contact the Web Guidelines team at the [ICT Branch](#).

### **2.4.4 Authentication standards**

Note: Agencies wishing to implement any new systems where authentication of individuals or businesses is necessary must contact the [ICT Branch](#) of the State Services Commission for advice.

#### **[Guide to Authentication Standards for Online Services](#)**

**Status** Under Development  
**Comments** An entry point and navigational tool for the suite of NZ e-GIF authentication standards

#### **[Evidence of Identity Standard](#)**

**Status** Under Development  
**Comments** Specifies a business process for establishing the identity of government agency customers.

#### **[Authentication Key Strengths Standard](#)**

**Status** Under Development  
**Comments** Specifies the requirements for the authentication keys and protections for the online authentication exchange.

**Data Formats for Identity Records Standard**

**Status** Under Development  
**Comments** Specifies a set of identity-related data elements that are presented in an agreed format, to provide a common approach for agencies to systemise their identity management processes for users of their services. The elements focus on 'who you are' (identity) rather than 'what you own/your role' (attributes of identity) or 'what you can do' (authorisation).

**Passwords Standard**

**Status** Under Development  
**Comments** Specifies the password requirements for online services in the Low Risk Category

**Security Assertion Messaging Standard (NZ SAMS)**

**Status** Under Development  
**Comments** Specifies a deployment profile of OASIS SAML v2.0 to communicate security assertions.



## 2.5 *Web Services layer*

Web Services is an emerging set of standardised applications to connect and integrate web-based applications over the Internet. The e-GIF identifies them separately, as they span multiple parts of the layer model. It is critical that agencies using web services agree on the implementation and semantics of data. The emergence of the [WS-I Basic Profile 1.1](#) offers a starting point for a consensus on implementing web services across government.

The following standards apply where systems use web services architecture.

### 2.5.1 **Discovery**

**[UDDI v3](#)**      **Universal Description, Discovery and Integration Version 3**  
**Status**        Adopted  
**Comments**    An open standard for describing, publishing, and discovering network-based software components.

### 2.5.2 **Description**

**[WSDL v1.1](#)**    **Web Services Description Language Version 1.1**  
**Status**        Adopted  
**Comments**    Specifies the location of the service and the operations, or methods, the service exposes.

**[WSDL v2.0](#)**    **Web Services Description Language Version 2.0**  
**Status**        Future Consideration

### 2.5.3 **Access**

**[SOAP v1.1](#)**    **Simple Object Access Protocol Version 1.1**  
**Status**        Adopted  
**Comments**    For Web Services Transport. E-GIF v3.1 recommends SOAP v1.2, but adopts SOAP v1.1 because of feedback from agencies that this is the version currently supported in many common development products.

**[SOAP v1.2](#)**    **Simple Object Access Protocol Version 1.2**  
**Status**        Recommended  
**Comments**    Previous versions of the e-GIF adopted SOAP v1.2. E-GIF v3.1 recommends SOAP v1.2, but adopts SOAP v1.1 because of feedback from agencies that this is the version currently supported in many common development products.

#### 2.5.4 Messaging

##### [ebXML MSG](#) **E-Business Extensible Markup Language Messaging Services**

**Status** Future Consideration

**Comments** Also known as ebMS.

##### [WSRM](#) **Web Services Reliable Messaging**

**Status** Future Consideration

**Comments** WS-Reliability 1.1 provides a standard, interoperable way to guarantee message delivery to applications or Web services

##### [AS2](#) **Applicability Statement 2**

**Status** Future Consideration

**Comments** A lightweight, open messaging transport for B2B messaging services. Comparable with ebXML MSG/ebMS.

#### 2.5.5 Security

##### [WSS](#) **Web Services Security**

**Status** Recommended

**Comments** A technical foundation for implementing security functions such as integrity and confidentiality in messages implementing higher-level Web services applications

##### [WS-Securitypolicy](#) **Web Services Security Policy Language**

**Status** Future Consideration

**Comments** This specification indicates the policy assertions that apply to Web Services Security: SOAP Message Security, WS-Trust, and WS-SecureConversation.

##### [WS-Trust](#) **Web Services Trust Language**

**Status** Future Consideration

**Comments** Uses the secure messaging mechanisms of WS-Security to define additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains.

##### [WS-Secon](#) **Web Services Secure Conversation Language**

**Status** Future Consideration

**Comments** The Web Services Secure Conversation Language (WS-SecureConversation) is built on top of the WS-Security and WS-Policy models to provide secure communication between services.

##### [SAML v1.1](#) **Security Assertion Markup Language Version 1.0**

**Status** Recommended

**Comments** Secure messaging and security token framework. See [Access and Presentation layer](#). [OpenSAML](#) is an implementation of SAML.

**[SAML v2.0](#) Security Assertion Markup Language Version 2.0**

**Status** Future Consideration

**Comments** Secure messaging and security token framework. A subset of SAML 1.1, elements are Under Development as part of the All-of-government Authentication project. See [Access and Presentation layer](#). [OpenSAML](#) is an implementation of SAML.

**[xACML v2.0](#) Extensible Access Control Markup Language Version 2.0**

**Status** Future Consideration

**Comments** XML Schema for creating policies and automating their use to control access to disparate devices and applications on a network.

**[Liberty ID-WSF v2.0](#) Liberty Alliance ID-WSF 2.0**

**Status** Future Consideration

**Comments** For consideration where app-to-app federated identity required and SAML V2.0 profiles not sufficient.

## 2.5.6 Compliance

**[WS-I Basic Profile v1.1](#) Web Services – Interoperability Organisation Basic Profile Version 1.1.**

**Status** Future Consideration

**Comments** Profiles provide implementation guidelines for how related web services specifications should be used together for best interoperability. To date, WS-I has finalised the Basic Profile, Attachments Profile and Simple SOAP Binding Profile.

**[WSS-I Basic Profile v1.0](#) Web Services Security – Interoperability Organisation Basic Profile Version 1.0.**

**Status** Future Consideration

**Comments** Draft 1.0 Basic Security Profile accepted by OASIS.

## 2.6 Security layer

Security is shown in the e-GIF as spanning all layers to reflect the fact that security needs to be designed into a system, not added as a layer on top. Security can be viewed in four main contexts:

- **Confidentiality:** Ensuring information is accessible only to those authorised to have access.
- **Integrity<sup>3</sup>:** Ensuring information has not been changed or altered without knowledge of this happening.
- **Availability:** Ensuring authorised users have access to information and associated assets when required.
- **Accountability:** A system's ability to keep track of who or what has accessed data, conducted transactions, or made changes to the system<sup>4</sup>.

Agencies are encouraged to consider the security implications of interoperability projects using these contexts, and apply the appropriate policies and standards. The following list contains standards designed to offer different levels of security in the layers; the standards and policy statements in the [NZSITs](#) provide advice and direction on what levels may be required.

Contact the [GCSB](#) where one or more of the systems exchanging information is likely to be carrying classified information (RESTRICTED or greater).

### 2.6.1 Policy

#### [GCSB NZSITs](#) Government Communications Security Bureau New Zealand Security of Information Technology Publications

**Status** Adopted

**Comments** Refer to the GCSB for advice on hashing, key transport, signing and cryptographic algorithms, as described in the current versions of NZSIT 400.

---

<sup>3</sup> Note: "Integrity" here does not refer to "data integrity", which is beyond the scope of the e-GIF. These standards are responsible for the integrity of the transport but not necessarily the integrity of the data.

<sup>4</sup> Sourced from ISO17799: IT - Code of Practice for Information Security Management.

**SIGS**            **Security in the Government Sector**  
**Status**            Adopted  
**Comments**        A manual of policies, principles and procedures mandated by Cabinet in 2001, developed using [AS/NZS ISO/IEC 17799:2001](#) - “Code of practice for information security management”.

Page 8-20, paragraph 10 of SIGS requires use of an IS framework following AS/NZS ISO/IEC 17799:2001 for all systems processing classified, including IN-CONFIDENCE, information or hosting government services.

Agencies should decide how much protection is required using the principles of general risk analysis and risk management found in AS/NZS 4360:1999 – “Risk Management”.

## 2.6.2        **Network**

**HTTPS**            **HyperText Transfer Protocol running over SSL**  
**Status**            Adopted  
**Comments**        See SSL v3 below.

**SSL v3.0**         **Secure Sockets Layer Version 3**  
**Status**            Adopted  
**Comments**        Use for encrypted transmission of any data quantity between web browser and web server over TCP/IP.

Used for HTTPS (HTTP in an SSL/TLS stream) to open a secure session on Port 443.

May also be used for secure TCP transport (e.g. VPN)

Note: TLS v1.0 is SSL v3.1

**IPsec**   **Internet Protocol Security**  
**Status**            Adopted  
**Comments**        Authentication header standard taken from NZSIT/SIGS.

**ESP**    **IP Encapsulation Security Protocol for VPN**  
**Status**            Adopted  
**Comments**        Requirements taken from NZSIT/SIGS.

**S-HTTP**         **Secure HyperText Transfer Protocol**  
**Status**            Future Consideration  
**Comments**        For individual messages, created by SSL running under HTTP.

**TLS v1.0**      **Transport Layer Security**  
**Status**          Future Consideration  
**Comments**      RFC 2616 upgrade mechanism in HTTP 1.1; initiate Transport Layer Security over an existing TCP connection. Does not yet interoperate with SSL v3.

### 2.6.3      **Data integration**

**XML - Enc**      **XML-Encryption syntax and processing**  
**Status**          Future Consideration  
**Comments**      Taken from [UK Technical Standards Catalogue Version 6.2](#).

**XML - DSig or OASIS DSS**  
**Status**          Future Consideration  
**Comments**      XML-Digital signature – syntax and processing as defined by W3C, used in SAML implementations. OASIS Digital Signature Services – developing an alternative implementation.

### 2.6.4      **Web services**

**SAML v2.0**      **Security Assertion Markup Language Version 2.0**  
**Status**          Future Consideration  
**Comments**      SAML V2.0 token profile V1.1 based on the OASIS Web Services Security standard stack. See [Access and Presentation layer](#).

#### **Security Assertion Messaging standard**

**Status**          Under Development  
**Comments**      All-of-government Authentication project standard Under Development. Expected to specify four specific messages from [SAML](#) for communicating authentication assertions.

### 2.6.5      **Business services**

**SEE PKI**      **Secure Electronic Environment Public Key Infrastructure**  
**Status**          Recommended  
**Comments**      For agencies using the [Secure Electronic Environment](#) (SEE) e-government component. See Section 3 [E-government Services](#) for more details.

**SEEMail**      **Secure Electronic Environment Mail**  
**Status**          Recommended  
**Comments**      A combination of procedures and standards already listed in the e-GIF, required to use the e-government component SEEMail service. See Section 3 [E-government Services](#) for more details.

**S/MIME v3.0 Secure Multi-Purpose Internet Mail Extensions Version 3**

**Status** Adopted

**Comments** Use MIME when security is not a concern. Use S/MIME encryption when not using the Messaging Transport protocols.

**SecureMail**

**Status** Under Development

**Comments** A draft RFC being developed by the ICT Branch of the State Services Commission, describing how to implement secure email between mail gateways using TLS.

**2.6.6 Public Key Infrastructure (PKI)**

**RFC2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework**

**Status** Recommended

**Comments** Produced by the Public-Key Infrastructure X.509 group, or PKIX, a working group of the Internet Engineering Task Force dedicated to creating RFCs and other standards documentation on issues related to public key infrastructure (PKI) based on X.509 certificates.

Note: Agencies wishing to implement any new PKI system must contact the ICT Branch of the State Services Commission for advice.

## 2.7 Best Practice layer

This section presents international standards and local conventions that support best practice, rather than the actual data exchange in interoperability. Agencies use these standards, not necessarily with direct dependence on the standards of other agencies with whom they interoperate, but to support interoperability in general.

### 2.7.1 Digital Rights Management (DRM)

**Status** Under Development

**Comments** Do not enable. See [October 2004 paper on Trusted Computing](#). A Working Group is considering conventions for use across government.

### 2.7.2 Trusted computing

**Status** Under Development

**Comments** A Working Group has developed a set of government-wide [principles and policies](#) for the use of trusted computing and digital rights management (TC/DRM) technologies in New Zealand. See also [SSC 2004 Report on Trust & Security](#).

### 2.7.3 Process

**[WSBPEL](#)** **Web Services Business Process Execution Language**

**Status** Future Consideration

**Comments** Lets users describe business process activities as web services and define how they can be connected to accomplish specific tasks.

**[FWSI](#)** **Framework for Web Services Implementation**

**Status** Future Consideration

**Comments** Defines methods and functional components for broad, multi-platform, vendor-neutral cross-industry implementation of Web services

**[CPPA](#)** **ebXML Collaboration Protocol Profile and Agreement**

**Status** Future Consideration

**Comments** Describing how trading partners engage in electronic business collaborations through the exchange of electronic messages

**[EBXML-BP](#)** **ebXML Business Process**

**Status** Future Consideration



**Comments** Providing a standards-based business process foundation that promotes the automation and predictable exchange of business collaboration definitions using XML

**BPEL4WS** **Business Process Execution Language for Web Services**

**Status** Deprecated

**Comments** Lets users describe business process activities as web services and define how they can be connected to accomplish specific tasks.

**2.7.4 XML data transformation**

**XSLT** **eXtensible Stylesheet Language Transformations**

**Status** Adopted

**Comments** A description vocabulary used by XSL to describe how an XML document is transformed into another XML document.

**XPath** **eXtensible Stylesheet Language Transformations**

**Status** Recommended

**Comments** XPath is a language for addressing parts of an XML document, designed to be used by both XSLT and XPointer.

**2.7.5 Data modelling**

**Entity Relationship Diagrams**

**Status** Adopted

**Comments** Useful for describing objects in a visual format.

**UML** **Unified Modelling Language**

**Status** Adopted

**Comments** Useful for describing objects in a visual format.

**XMI** **XML Metadata Interchange**

**Status** Recommended

**Comments** Enables easy interchange of metadata between modelling tools such as UML and remote metadata repositories.

**UBL** **Universal Business Language**

**Status** Future Consideration

**Comments** Naming and design rules for schema design.

**2.7.6 Processing structured data**

**SAX** **Simple API for XML**

**Status** Adopted

**Comments** Parser for large volume repetitious batch transfers. Open standard for navigating and updating XML documents.

**DOM Document Object Model**

**Status** Recommended

**Comments** Parser for transactional exchanges. SAX is a Java API for navigating XML documents.

**XQuery 1.0 XML Query Language**

**Status** Future Consideration

**Comments** A query language that can express queries across diverse data sources including structured and semi-structured documents, relational databases, and object repositories, whether physically stored in XML or viewed as XML via middleware.

**XLink 1.0 XML Linking Language**

**Status** Future Consideration

**Comments** A linking language that allows elements to be inserted into XML documents in order to create and describe links between resources.

**2.7.7 Controlled Vocabulary or code Lists (CVLs)**

**Status** Future Consideration

**Comments** Discussion on [standardising CVLs](#). Research underway, led by the ICT Branch of the State Services Commission.

**2.7.8 Health sector**

**HL7 Health Level 7**

**Status** Under Development

**Comments** An international standard adopted by the health sector. Is converging on HL7 Version 2.4 for laboratory results and National Health Index (NHI).

**2.7.9 Document file format**

**ODFOA v1 Open Document Format for Office Applications Version 1  
DocBook, DocBook**

**Status** Future Consideration

**Comments** Several candidates for agencies to save documents in an open, XML format.

#### **2.7.10 Biometrics**

##### **ISO/IEC 19794 - Parts 2-6:2005 Information technology – Biometric data interchange formats**

**Status** Future Consideration

**Comments** Applying to access control, ID systems and storage on databases. (Ref Mark Tesoriero at Customs for guidance).

Note that biometrics are specifically prohibited for transmission with an online transaction (Cabinet Minute EXG (03) 37 24th June 2003)

#### **2.7.11 Evidence collection**

##### **HB 171-2003 Guidelines for the management of IT evidence**

**Status** Future Consideration

**Comments** Provides useful guidelines for agencies in management of evidence held in computerised systems.

#### **2.7.12 Business Transactions**

##### **UBL Universal Business Language**

**Status** Future Consideration

**Comments** Defining a common XML library of business documents (purchase orders, invoices, etc.)

### 3 E-government Services

The following items comprise the E-government Services. They are actual implementations of useful functions that are:

- available for re-use by public sector agencies
- compliant with the e-GIF.

The items are:

- **Metalogue:** [Services and Document Description \(metadata\) Database](#)
  - A web-based repository for metadata, used to drive the Portal.
- **Portal News Feed:** [News Syndication](#)
  - Uses NZ Government RSS to accept news items from government agencies for display on the Portal. This can also provide a feed of government news for use on agency websites.
- **Authentication:** [Government to Individual and Government to Business online authentication](#)
  - The Government Logon Service (GLS) is currently available for implementation by agencies. It provides affordable access to high-quality authentication services. The GLS provides people with a common logon, such as a username and password or token, to access all online services provided by participating agencies.
- **Shared Workspace:** [Online collaboration tool](#)
  - Workspace is available at a modest charge for agencies to run collaborative projects in an online environment. Workspace content-management functionality includes message threading, library and archiving, alerting and news/event announcements.
- **Public Sector Intranet:** All-of-Government online information repository
  - The Public Sector Intranet was launched as a full production system, in June 2006. For more information, contact [mailto: PSI@ssc.govt.nz](mailto:PSI@ssc.govt.nz).
- **SEEMail:** New Zealand Government Secure Email system; [SEEMail](#)
  - SEEMail is a gateway-gateway crypto layer running over public email, improving confidentiality and authentication. It is intended for use between government bodies (including local government). Note the next version of this service will not accept UUENCODE or TNEF message formats.
- **Search Engine:** Autonomy search engine (Deprecated)

- Please note that government agency web search capability is under review. Agencies considering products are advised to contact the [ICT Branch](#).
- **Government Shared Network:** [modular structured network that will enable government agencies to share information at higher speeds and more cost effectively](#)
  - The Government Shared Network is a secure network linking government agencies with high-speed Internet and telecommunications services. The initial set of services is being deployed by early adopting agencies at the end of 2006, with general release in early 2007.
  - The Government Shared Network (GSN) features a fully managed infrastructure, with a 24 x 7 Service Desk. Contact <mailto:gsn@ssc.govt.nz>.

STATE SERVICES COMMISSION  
Te Kōmihana O Ngā Tari Kāwanatanga



**New Zealand E-government  
Interoperability Framework  
(NZ e-GIF)**

**Version 3.1**

**PART 2 – POLICY**

**November 2006**

State Services Commission

Te Kōmihana O Ngā Tari Kāwanatanga

## **About this document**

This document outlines the policy behind the e-GIF and its development. The intended audience for this Policy section includes:

- policy analysts
- advisors
- business analysts
- anyone involved with interoperability strategy and projects.

It includes the following sections:

- [What is the e-GIF?](#) Short descriptions of e-government, interoperability, and the e-GIF, how the e-GIF will benefit New Zealand, and how the e-GIF is maintained.
- [Who must comply and when?](#) Who must comply with the e-GIF, how to transition to e-GIF compliance, exemptions and special provisions.
- [Principles](#): Short descriptions of anticipated outcomes of the e-GIF, requirements for project and operational management, and governance principles.
- [Developing the e-GIF](#): Outlines of procedures for extending the e-GIF, submitting a new standard, developing the framework, and issues under review or proposed for future working groups.

## Table of Contents

<b>1</b>	<b>What is the e-GIF?</b> .....	<b>1</b>
1.1	What is e-government? .....	1
1.2	What is interoperability?.....	Error! Bookmark not defined.
1.3	What will the e-GIF accomplish? .....	2
1.3.1	Practical example: Consolidating customer resources.....	3
1.4	Managing the e-GIF .....	4
1.4.1	Stewardship .....	4
1.4.2	Who to contact .....	4
<b>2</b>	<b>Who must comply and when?</b> .....	<b>5</b>
2.1	Who must or is encouraged to comply .....	5
2.1.1	Mandatory compliance.....	5
2.1.2	Suggested compliance.....	5
2.2	How and when to comply .....	6
2.2.1	Transitions.....	6
2.2.2	Information sharing and matching agreements .....	6
2.3	Exemptions .....	7
2.3.1	Special provisions .....	8
<b>3</b>	<b>Principles</b> .....	<b>9</b>
3.1	Outcomes for government .....	9
3.2	Aims of the e-GIF .....	10
3.2.1	Improving the public face of government.....	10
3.2.2	Improving agency use of ICT .....	10
3.2.3	Operating in a global environment.....	10
3.3	Governance of shared inputs .....	11
3.3.1	Project management .....	11
3.3.2	Operational management .....	11
3.4	Governance principles .....	11
<b>4</b>	<b>Developing the e-GIF</b> .....	<b>13</b>



**e-GIF Version 3.1**  
**PART 2 - POLICY**

<b>4.1</b>	<b>How to extend the e-GIF .....</b>	<b>13</b>
<b>4.2</b>	<b>Submitting a new standard .....</b>	<b>13</b>
<b>4.3</b>	<b>Principles for developing the framework.....</b>	<b>13</b>
<b>4.4</b>	<b>Alignment with other framework initiatives .....</b>	<b>14</b>
<b>4.5</b>	<b>Issues under review .....</b>	<b>14</b>

## 1 What is the e-GIF?

The E-government Interoperability Framework (e-GIF) is a set of policies, technical standards, and guidelines. It covers ways to achieve interoperability of public sector data and information resources, information and communications technology (ICT), and electronic business processes. It enables any agency to join its information, ICT or processes with those of any other agency using a predetermined framework based on “open” (i.e. non-proprietary) international standards.

While a universally agreed definition of "open standards" is unlikely to be resolved in the near future, the e-GIF accepts that a definition of “open standards” needs to recognise a continuum that ranges from closed to open, and encompasses varying degrees of "openness". To guide readers in this respect, the e-GIF endorses "open standards" that exhibit the following properties:

- **Be accessible to everyone free of charge:** no discrimination between users, and no payment or other considerations should be required as a condition to use the standard.
- **Remain accessible to everyone free of charge:** owners should renounce their options, if any, to limit access to the standard at a later date.
- **Be documented in all its details:** all aspects of the standard should be transparent and documented, and both access to and use of the documentation should be free.

The e-GIF performs the same function in e-government as the Road Code does on the highways. Driving would be excessively costly, inefficient, and ineffective if road rules had to be agreed each time one vehicle encountered another.

### 1.1 What is e-government?

E-government is about government agencies working together to use technology so they can better provide individuals and businesses with government services and information. It is not a massive ICT project. Much of it is about establishing common standards across government, delivering services more effectively, and providing ways for agencies to work together using technology.

E-government presents New Zealand with some tremendous opportunities to develop higher quality, cost-effective, government services and a better relationship between New Zealanders and their government.

For the latest version of the New Zealand E-government Strategy, see <http://www.e.govt.nz/about-egovt/strategy/nov-2006/>

## **1.2 What is interoperability?**

The December 2001 [E-government Strategy Update](#) defines interoperability as “the ability of government organisations to share information and integrate information and business processes by use of common standards”.

The June 2003 [E-government Strategy Update](#) underscores this point: “Common data and information technology policies and standards underpin the service delivery architecture and are integral to the E-government Strategy.”

The November 2006 [E-government Strategy Update](#) “confirms the key role of collaboration, standards and interoperability, and an enterprise architecture for government in achieving the Strategy's goals.” It defines Building Standards and Interoperability as “Government adopting and using common standards to ensure agencies and their partners can work together, and users can access government services and information”.

From a technical standpoint, interoperability is achieved when the coherent, electronic exchange of information and services between systems takes place.

For e-government in New Zealand, interoperability relates specifically to the electronic systems that support business processes between:

- agencies
- government and people
- government and business.

This does not mean a central agency is simply dictating common systems and processes. Interoperability can be achieved by applying a framework of policies, standards and guidelines that leave decisions about specific hardware and software solutions open for individual agencies, or clusters of agencies, to resolve.

This document sets out this framework.

## **1.3 What will the e-GIF accomplish?**

Using the e-GIF will:

- help government agencies to work more easily together electronically
- make systems, knowledge and experience reusable from one agency to another
- reduce the effort needed to deal with government online by encouraging consistency of approach

- reduce the reliance on tapes and disks to exchange data, as these carry their own security issues and are not scaleable for the level of interoperability many services will need in future.

### 1.3.1 Practical example: Consolidating customer resources

Adhering to the e-GIF becomes critical when two or more agencies work together to deliver a service online. Agencies in this situation are encouraged to look at services from a “customer” perspective.

A hypothetical example is opening a café or restaurant. At present, this involves interactions with a number of agencies:

- The Companies Office and Inland Revenue, which provide a shared service for people wanting to start a business. As people incorporate their company, they are able to apply for an IRD tax number. By entering information into the “IRD Details” screen during the online company incorporation process, their application will be sent via an automated link to Inland Revenue. (Until recently new companies had to deal with the Companies Office and Inland Revenue separately).
- Occupational Safety and Health ([OSH](#)) for accident forms, hazardous substances policy, etc.
- Accident Compensation Commission ([ACC](#)) for levy forms and workplace safety policy, etc.
- The local council for signage, a certificate of food hygiene, etc.

At present, most of this information is available online, but only by visiting each agency’s website for its respective services.

Consider this example in an interoperable future: all services for opening a café or restaurant, delivered by multiple agencies, available through a single website: <http://www.openingmycaferestaurant.govt.nz>. The applicant would enter relevant details, then the agencies would exchange relevant information among themselves and the applicant to supply all the required services.

This is the kind of interoperability envisaged in the next phase of e-government. To achieve such interoperability, the agencies need an enduring, agreed set of standards for exchanging data between all parties. The e-GIF sets out these standards.

(See also Section 3.2, [Aims of the e-GIF](#).)

## 1.4 *Managing the e-GIF*

### 1.4.1 Stewardship

The following people manage the e-GIF:

- The **State Services Commissioner** is the **Steward** of the e-GIF, with accountability and corresponding decision-making authority for its ongoing development and management.
- The **Information and Communication Technologies Branch (ICT Branch)**<sup>1</sup> of the State Services Commission is the **Custodian**, with responsibility for the day-to-day operation of the e-GIF under the oversight of the e-GIF Management Committee.
- The **e-GIF Management Committee** is made up of public servants from the senior ranks of agencies adopting the e-GIF. The Committee acts for the State Services Commissioner to ensure:
  - the value of the e-GIF as a “collective asset” that supports the future capability and performance of both individual agencies and the public sector as a whole, and one that is maintained and enhanced across time
  - the benefits of the e-GIF (increased agency and public sector capability, performance, efficiency and effectiveness) outweigh its costs (decreased agency-level autonomy, administration costs, etc.).
- **Working Groups** are established to regularly review the technical aspects of the e-GIF.
- All **agencies** that are required to adopt the e-GIF may take part in its governance and appeal decisions made by the Steward and Management Committee.

### 1.4.2 Who to contact

You can contact the Custodian at [e-gif@ssc.govt.nz](mailto:e-gif@ssc.govt.nz).

---

<sup>1</sup> The Information and Communication Technologies Branch (ICT Branch) of the State Services Commission, was formed from the E-government unit on 1 July 2005.

## 2 Who must comply and when?

The e-GIF is a forward-looking document. It specifies a set of standards to be applied when developing or upgrading technology. This section outlines who must and who is encouraged to comply, how to make the transition, and how to apply for an exemption.

### 2.1 *Who must or is encouraged to comply*

#### 2.1.1 **Mandatory compliance**

From 1 July 2002, Cabinet has made using the e-GIF **mandatory** for:

- all Public Service departments
- the New Zealand Police
- the New Zealand Defence Force
- the Parliamentary Counsel Office
- the Parliamentary Service
- the Office of the Clerk
- the New Zealand Security Intelligence Service.

#### 2.1.2 **Suggested compliance**

The benefits of the e-GIF are not specific to the Public Service or central government. Cabinet has **encouraged** adoption by:

- organisations in the wider State sector
- local authorities.

The e-GIF is also open to use by:

- non-government organisations
- the business community
- the public
- other jurisdictions.

## **2.2 How and when to comply**

In general, all organisations that must or are encouraged to comply with the e-GIF (see Sections 2.1.1 and 2.1.2), should review their implementations against the e-GIF whenever:

- a new version of the e-GIF is released
- they are contemplating new implementations
- they are contemplating upgrading implementations, and/or
- they are reviewing their overall technology strategy.

See the following sections for details.

### **2.2.1 Transitions**

The adoption of the e-GIF must allow for a sensible transition. Recognising this, Cabinet agreed on 13 June 2002 that current information systems, software applications, or electronic data/information resources did not need to comply immediately with the e-GIF.

Any **new** information system, software application, or electronic data/information resource (or current instances of these being redeveloped or replaced), or systems for interfacing with these, must comply with the e-GIF except where:

- it is certain that interoperability will never be a requirement, or
- the current version of the e-GIF does not, and could not, include policies, standards or guidelines concerning the technologies the agency needs (not wants) to employ.

If an agency has one of these exceptional instances, it needs to consider the customer perspective (see Section 1.3.1). Although the agency system may have been developed to operate in isolation, New Zealanders may one day need it, transparently or otherwise, to work with other services from other agencies. Is it certain that the new system, application or resource will never need to support or interact with any new, enhanced, or replacement system, application, interface, service, process, or resource? Experience shows that in most cases, the e-GIF will apply.

### **2.2.2 Information sharing and matching agreements**

In many, but not all, circumstances, interoperability requires the exchange, sharing, or matching of personal information. The [Privacy Act](#) may well apply in these situations, particularly Part 10 and schedules 3 and 4. For information-matching programmes, the Act mandates a Technical Standards Report.

Agencies planning data exchange are encouraged to:

- contact the [Office of the Privacy Commissioner](#) about the circumstances of the exchange (it may fit with one of the information-matching programmes authorised by Parliament)
- review their existing (offline) data management agreements and:
  - extend them to include issues relating to electronic exchange
  - add them to the Technical Standards Report or
  - prepare new agreements or Memoranda of Understanding
- seek legal advice.

See also:

- Section 3.3 Governance of shared inputs.
- Part 3, [Section 1.10](#) Information Systems and Data Management Policies and Standards.
- Checklist for data exchange issues to be covered in a Memorandum of Understanding (MOU) or data sharing agreement. Please email [e-GIF@ssc.govt.nz](mailto:e-GIF@ssc.govt.nz) for access to this document.

### **2.3 Exemptions**

Where an agency believes there are grounds for exemption from the e-GIF, it must:

- conclusively demonstrate, to the satisfaction of the e-GIF Steward, where the current version of the e-GIF cannot meet requirements or why an alternative approach to achieving interoperability is justified
- where sensible, contribute to updating the e-GIF.

Where an exemption is approved, it will apply only to a specific:

- information system, software application, data/information resource, or business process (not to the agency's entire information and technology environment and/or business processes)
- agency or agencies (not to an entire sector)
- time period (not indefinitely).

For more information, including a template for applying for an exemption, see <http://www.e.govt.nz/standards/e-gif/faqs.html>.



### **2.3.1 Special provisions**

Specialist systems employed, or sponsored, by the security and intelligence agencies are automatically exempted where it is not appropriate for them to comply with the e-GIF.

## 3 Principles

### 3.1 Outcomes for government

The e-government programme seeks the following outcomes, which will be helped by applying the e-GIF:

- **Convenience and satisfaction:** Services provided anytime, anyhow, anywhere; people will have a choice of channels to government information and services that are convenient, easy to use, and deliver what is wanted. This outcome will be achieved when:
  - many services are fully or partially delivered electronically (as appropriate)
  - traditional service delivery channels (counter, postal, telephone, etc.) continue to exist but are enhanced by the use of technology.

By interoperating using the e-GIF, agencies will provide services and information electronically in the way that people want.

- **Integration and efficiency:** Services that are integrated, customer-centric and efficient; information and services will be integrated, packaged, and presented to minimise cost and improve results for people, businesses, and providers. This outcome will be achieved when:
  - front-office integration is well developed, with many services redesigned and bundled together in ways that better meet customer needs
  - back-office integration is advancing through adopting the e-GIF and progressively building components of the service delivery architecture.

By interoperating using the e-GIF, agencies can work together electronically, acting more like a single enterprise than a collection of individual agencies.

- **Participation:** People will be better informed and better able to participate in government. This outcome will be achieved when:
  - online participation becomes an increasingly important part of policy development and service delivery
  - democratic processes may be electronically enabled (e.g. e-voting in local body elections).

By interoperating using the e-GIF, agencies can make information available to people in ways that help them to participate in the processes of government.

## **3.2 Aims of the e-GIF**

The e-GIF aims to improve the practical application of information and communications technologies (ICT) between the public and government, within and between agencies, and within a global context.

### **3.2.1 Improving the public face of government**

People generally access government services out of need rather than choice. Their needs are seldom confined to the business of a single agency. Rather, people typically have to deal with several agencies to achieve their goals or meet their obligations.

One of the aims of the e-government programme is to make it easier for people to deal with multiple agencies by making good use of ICT. By making ICT systems and the processes they support interoperate, people will find it easier to do business with government as a whole. This does not mean that everyone has to be online to benefit from interoperability. If agency ICT is interoperating effectively, people dealing with public servants face-to-face or on the phone will also receive better service.

### **3.2.2 Improving agency use of ICT**

Adopting common technical standards for ICT means agencies can focus more on the business outcomes the systems are designed to support rather than on technical choices that have little impact on service delivery.

Common technical standards also mean the collection of ICT systems across government is more valuable than the sum of its parts. Disparate systems that cannot work together are only valuable in and of themselves.

Adopting common technical standards also means that, across government, knowledge of these technologies will be concentrated rather than spread across numerous alternative and often proprietary technologies.

### **3.2.3 Operating in a global environment**

The Internet, and the value it can deliver to government and people, relies on an agreed, standards based approach. By using the same standards based approach, agencies support the infrastructure of technologies that they increasingly rely on to deliver services and conduct the business of government.

Adopting common standards also helps governments in various jurisdictions to interoperate. This becomes important when dealing with matters that can only be handled in a regional or global way.

### **3.3 Governance of shared inputs**

Agencies interoperate to:

- make better use of information and communications technologies (ICT) within government
- deliver an integrated service directly to people or business.

In both cases, collaborating agencies jointly provide inputs and must allocate the decision-making rights accordingly. Guidance on how to go about allocating decision-making rights is available from the [ICT Branch of the State Services Commission](#).

#### **3.3.1 Project management**

Before committing significant expenditure on an initiative involving more than one agency, those involved should agree and put in place appropriate project management processes (see “[Guidelines for Managing and Monitoring Major IT Projects](#)”).

#### **3.3.2 Operational management**

There should be some form of agreement for the ongoing operation of any initiative involving more than one agency. The content of the agreement will depend on the nature of the initiative, but the following areas should be considered:

- roles and responsibilities of each agency
- processes undertaken by each agency and the required service levels
- performance measurement for each agency’s service and problem resolution
- data quality and problem resolution
- cost recovery between agencies.

### **3.4 Governance principles**

The following principles underpin the governance of the e-GIF and its operation:

- The e-GIF will align with the [E-government Strategy](#) and the recommendations of the [Review of the Centre](#).
- There will be a clear chain of accountability flowing from a Cabinet Minister with appropriate portfolio responsibilities.
- Adequate organisational resources and capabilities must support the governance arrangements.

- The governance arrangements will be consistent with public sector legal requirements.
- The principles of stewardship and custodianship apply, as set out in the [Policy Framework of Government-held Information](#) [CAB (98) M 22/27 refers].
- Roles, responsibilities, and accountabilities will be clear.
- The governance arrangements will build confidence in, and commitment to, the e-GIF from all its stakeholders.
- With regard to the day-to-day operation of the e-GIF, the governance arrangements will show a close fit with the responsibilities and capabilities of the organisations involved.
- The processes for maintaining, developing, and implementing the e-GIF should be inclusive and as consensual as possible.
- The governance arrangements must account for the complexity of e-government stakeholders and operating environments.
- Agencies that are required to adopt the e-GIF will be given the opportunity to take part in its governance.
- Agencies that are required to adopt the e-GIF will have access to a process for raising concerns over decisions made by the Steward or the Management Committee.
- The collective interests of government should be balanced with the interests of individual agencies and their stakeholders. Where this is not possible, the collective interest should be given greater priority.
- Decision-making processes will be transparent.

## 4 Developing the e-GIF

### 4.1 *How to extend the e-GIF*

The Custodian and Steward of the e-GIF encourage agencies to submit technical standards, especially schemas that have been developed for an agency's specific business needs or for the needs of several agencies in a sector or area of business.

Including these in the framework ensures such standards are widely recognised in the New Zealand public sector and can be applied, where appropriate, to meet business needs elsewhere in the sector.

The governance processes put in place for the e-GIF aim to balance the collective interest of government with the interests of individual agencies and their stakeholders. Where this is not possible, collective interest should be given greater priority.

### 4.2 *Submitting a new standard*

The e-GIF is regularly reviewed and updated by issuing a revised version of this document. However, extensions to the e-GIF can be suggested at any time. This should be done by first contacting [e-gif@ssc.govt.nz](mailto:e-gif@ssc.govt.nz).

Proposed extensions will be reviewed by working groups that advise the e-GIF Custodian. The Custodian makes recommendations to the e-GIF Steward, through the e-GIF Management Committee.

Agencies that are required to adopt the e-GIF may appeal decisions to the Management Committee.

The standards submission process, together with a template to propose a new standard, can be found at <http://www.e.govt.nz/standards/e-gif/faqs.html>. Note that the agency proposing the standard is expected to take a share in the development and governance of the standard.

### 4.3 *Principles for developing the framework*

As well as the [principles](#) outlined in this document, a number of guiding principles have been developed for the long-term. For further information email [e-gif@ssc.govt.nz](mailto:e-gif@ssc.govt.nz).

#### **4.4 Alignment with other framework initiatives**

Open standards feature strongly in the e-GIF. [OASIS](#), [W3C](#), [ISO](#) and other standards organisations are developing standards with a global user base in mind.

The New Zealand e-GIF also draws from other jurisdictions, most notably the United Kingdom and Australia.

Agencies and service sectors are encouraged to draw from open standards to facilitate a greater level of uptake for bundled services in the future.

#### **4.5 Issues under review**

The 2005 e-GIF Review Group recommended the following strategies for further developing the e-GIF:

- **Extending the layer model:** The layer model ([See Part 1, Section 1.1](#)) categorises the technology standardised by the e-GIF structurally but not functionally. In practice, standards have a context. Some standards may only work in a particular situation or for a particular domain, or depend on the use of other standards, or represent high level aggregations of lower level components. One possibility is to include additional descriptions to the standards, such as “applicable to”, “used by”, “used with”, “pre-requisites” and/or “relies on”. Another possibility is to create an additional category, or layer, for the emerging use of implementation profiles for XML-based standards.
- **Changing Recommended (R) to Emerging (E):** There is some confusion about the word “Recommended” in the current e-GIF compliance status levels ([see Part 1, Section 1.3](#)). For example, a new version of a product might be better, therefore recommended, but actually less interoperable until more agencies use it. Ultimately, we would like to see the new version used, and therefore we recommend it when upgrading. Another ambiguity is that some may believe that if a standard is “Adopted”, it is the standard and, therefore, why would another be “Recommended”? To address these concerns, another word such as “Emerging” might replace “Recommended” in future for this status level.
- **Adding review cycle information:** Since standards proceed through a cycle of compliant statuses, review cycle information could be included to indicate how long each standard is in force and when it is due for review.
- **Continuous review cycles:** With technology changing constantly, the e-GIF needs to be updated continuously to remain relevant.
- **Using [RFC 2119](#):** This RFC could be used to clarify the interpretation of key words related to the standards. It standardises use of the words “must”,

“must not”, “required”, “shall”, “shall not”, “should”, “should not”, “recommended”, “may”, and “optional” when specifying requirement level.





**New Zealand E-government  
Interoperability Framework  
(NZ e-GIF)**

**Version 3.1**

**PART 3 – RESOURCES**

**November 2006**

State Services Commission

Te Kōmihana O Ngā Tari Kāwanatanga

## **About this document**

This document contains resources related to the e-GIF. The intended audience for this Resources section is all readers of the e-GIF.

It includes the following sections:

- [History of the e-GIF](#): Review of stages in the e-GIF's development, including a Change Log.
- [References and background information](#): Descriptions and links to further information related to the e-GIF.
- [URLs referred to in the e-GIF](#): Full URLs for all hyperlinks in the e-GIF.
- [Abbreviations](#): Definitions of abbreviations and acronyms used in the e-GIF.

## Table of Contents

<b>1</b>	<b>History of the e-GIF .....</b>	<b>1</b>
1.1	The UK e-GIF .....	1
1.2	NZ e-GIF v1 .....	1
1.3	Current NZ e-GIF .....	1
1.4	Change Log.....	1
<b>2</b>	<b>References and background information .....</b>	<b>8</b>
2.1	E-government Strategy .....	8
2.2	Policy Framework for Government-held Information .....	8
2.3	Privacy Act 1993 .....	8
2.4	Security in the Government Sector .....	8
2.5	Information Systems and Data Management Policies and Standards .....	8
	<b>URLs referred to in the e-GIF .....</b>	<b>9</b>
2.6	Standards.....	10
2.7	e-GIF documents .....	18
2.8	Other New Zealand Government documents .....	18
2.9	Other resources .....	19
<b>3</b>	<b>Abbreviations.....</b>	<b>20</b>



## 1 History of the e-GIF

### 1.1 *The UK e-GIF*

The original version of the NZ e-GIF was based on work done by the [Office of the UK e-Envoy](#) in producing the UK e-GIF, which was first published in 2000. The UK e-GIF was reviewed by working groups comprising agency and vendor representatives, during the latter part of 2001.

### 1.2 *NZ e-GIF v1*

Version 1 of the NZ e-GIF was published in May 2002, incorporating feedback from some 25 agencies. The following month, Cabinet agreed the NZ e-GIF would govern how public sector organisations achieved electronic interoperability of their information, technology and business.

### 1.3 *Current NZ e-GIF*

The current version of the e-GIF is available at <http://www.e-gif.govt.nz>. All major revisions to the e-GIF supersede earlier versions.

### 1.4 *Change Log*

#### 1.4.1 **Version 3.1 – 21 November 2006**

This version has minor updates to the e-GIF. In particular, it has:

- added Government Shared Network section
- updated references within the following sections: Trusted Computing, Authentication, Uniform Resource Name (URN), Network Time Protocol (NTP), Universal Time Clock (UTC), Public Sector Intranet (PSI), Name and Address, E-learning
- updated references to the Web Guidelines, to reflect the latest version
- updated references to the E-government Strategy, to reflect the latest version
- updated Open Document references
- added Security Assertion Messaging standard (NZ SAMS)
- added Digitalisation standard

#### **1.4.2 Version 3.0 - 3 June 2005**

This version is a substantial rewrite of the e-GIF to make it clearer and broader. In particular, it has:

- restructured the document, separating Standards, Policy, and Appendixes (Resources)
- added general information about e-government, interoperability, and the e-GIF
- clarified how to comply and included the requirement for data share agreements
- added agency and time limitations to exemption requirements
- revised the layer model to:
  - add Best Practice
  - separate out Web Services
  - change “Architecture” to “Data Integration”
  - change “E-government Component Architecture” to “E-government Services” and put it in a separate section
- changed “categories” to “compliant status levels”, added new status classifications (**F, U, R, A, D**), diagram, and explanations
- added links to standards, procedures for submitting standards and applying for exemptions, the Roadmap for the e-GIF, and other resources on the Internet
- restructured list of standards and added comments
- added, moved, removed, or revised the following standards:
  - Network protocols (TCP/IP), UDP
  - File transfer protocols, WebDAV, SCP
  - Registry services (renamed, was “Registers”), DNS
  - Time, NTP, UTC (MSL)
  - Messaging transport, HTTP 1.1
  - Messaging formats, MIME
  - Primary character set, ASCII
  - Document type definition, DTD
  - Batch/bulk data, CSV

- File compression, GZIP
- File archiving, TAR
- Namespace, URN, OIDS
- Customer relationship, xCRL
- E-learning, ADL, SCORM, and IMS
- Business reporting, xBRL
- Directory services, DSML
- Statistical data and metadata, SDMX
- Geospatial, NZGMS
- XML 1.1
- Web services, all components, all standards
- Instant messaging, XMPP
- Voice Over Internet Protocol, SIP, RTP, H.323, G.711, G.729
- Web site presentation, NZ Govt Web Guidelines Version 2.1
- Forms, xForms
- Additional customer information, xCIL, Data formats for identity records standard
- Security (re-sorted components by layer model) - Network, HTTPS, S-HTTP, TLS, IPsec, ESP
- Data integration, XML – Enc
- XML – Dsig or OASIS DSS
- Web services, SAML v2.0, Shared Logon assertion messaging standard
- Shared Workspace
- Government Intranet
- SecureMail
- Best Practice, all components, all standards, added section
- moved the following standards:
  - UDDI, moved to Web Services / Discovery

**e-GIF Version 3.1**  
**PART 3 - RESOURCES**

- ebXML, moved to Web Services / Messaging
- Structured data description, RDF, moved to Business services
- Metadata (Discovery), NZGLS 2.0, NZGLS Thesauri, moved to Business services
- Unicode, moved; Comment: an extension of ASCII
- Graphics File, GIF89a, JPG, PNG, SVG, moved to Access and Presentation / Website presentation
- Mail Attachment, MIME, moved to Network / Messaging formats
- S/MIME, moved to Security / Business services
- XSLT, moved to Best Practice / XML data transformation
- UML, XMI, moved to Best Practice
- Business services, Metadata (Discovery), RDF, moved from Network / Structured data description
- Business services (continued), Presentation, GIF89a, JPG, PNG, SVG, PDF, moved to Access and Presentation / Website presentation
- Structured data description, RDF, moved to Metadata (Discovery) component
- UML, XMI, moved to Best Practice
- SOAP 1.2, moved to Web Services / Access
- General Text and Graphics, HTML v4.01, GIF89a, JPG, PNG, SVG, PDF, moved to Website presentation (comment)
- UDDI, moved to Web Services / Discovery
- WSDL 1.1, moved to Web Services / Description
- Processing (Structured data), SAX, DOM, renamed, was “Modelling (Structured Data)”, moved to Best Practice
- removed the following standard:
  - Autonomy
- revised the following standards:
  - Data integration, renamed, was “Architecture”



- Structured web document language, HTML v4.01, renamed component, was “Hypertext”
- Name and address, xNAL v2, specified version
- Registry services, renamed, was “Registers”, ebXML RIM and RS v2.1 and v3.0, specified versions
- E-government Services, renamed, was “E-government Component Architecture”
- Content syndication and channel feeds, RSS, renamed component, was “News Syndication”
- Authentication standards, Evidence of identity, Username / passwords, “Key type 2”, Authentication key strengths, Trust levels for online transactions, spelled as out separate standards
- Business services, S/MIME v3 , specified version.

#### **1.4.3 Version 2.1 - 14 May 2004**

- NZ xNAL schema added to Recommended to clarify the standard.

#### **1.4.4 Version 2.0 - 1 December 2003**

This was a substantial rewrite of the e-GIF to clarify its intent and make it more accessible. In particular it:

- introduced a new layer model and removed the old one
- removed the old divisions of Interconnection, Information Sharing and Exchange, Access, and Service Delivery and reclassified standards into Network, Architecture, Business Services, and Access and Presentation
- added a list of e-Government components
- replaced the terms Standards and Guidelines with Mandatory and Recommended to clarify intent
- reclassified all standards in the move to version 2; in addition, the status of the following standards was changed:
  - promoted PNG (portable network graphics) to an option in the Mandatory class (others were GIF and JPG) due to maturity of the standard.
  - corrected XSL to XSLT under data transformation services.
  - added version number on ZIP compression standard – now ZIP 2.3.
  - added xNAL as Mandatory standard for Name and Address data transfers.
  - made SAX a Mandatory standard (was a guideline, now called Recommended) for modelling structured data.
  - added New Zealand Government RSS as a future standard for news syndication.
  - added a placeholder for authentication standards with a note to seek EGU advice.
  - updated reference to New Zealand Government Web Guidelines to current version (v2.1).
  - added note about SecureMail as potential future government-to-citizen hardened email standard.
  - added lists of EGU components – available and under development.

**1.4.5 Version 1.1 - 3 July 2003**

Added ESA as a Recommended standard.

**1.4.6 Version 1.0 - 13 June 2002**

Initial release of e-GIF.

## 2 References and background information

### 2.1 *E-government Strategy*

The E-government Strategy is periodically reviewed and updated. The current version of the strategy can be found at <http://www.e.govt.nz/about-egovt/strategy>

### 2.2 *Policy Framework for Government-held Information*

All aspects of the [Policy Framework for Government-held Information](#) apply to data and information that is shared, exchanged, or otherwise used or managed under the specifications or coverage of the e-GIF. This requirement extends to the e-GIF itself.

### 2.3 *Privacy Act 1993*

The development and application of the e-GIF must comply with the [Privacy Act](#).

### 2.4 *Security in the Government Sector*

The development and application of the e-GIF must comply with the manual, [Security in the Government Sector](#).

### 2.5 *Information Systems and Data Management Policies and Standards*

While the e-GIF applies when agencies share information, technology and business processes, the Information Systems and Data Management Policies and Standards provide good-practice guidance for internal aspects of agency information and technology management:

<http://www.e.govt.nz/standards/e-gif/data-management-policies>

<http://www.e.govt.nz/standards/e-gif/data-management-standards>

<http://www.e.govt.nz/standards/e-gif/is-policies-standards>

## **URLs referred to in the e-GIF**

This document refers to a range of resources on the Internet, including:

- standards
- e-GIF documents
- other New Zealand Government documents
- other resources.

These links are listed in full in the following sections.

## **2.6 Standards**

### **AS2**

<http://www.ietf.org/rfc/rfc4130.txt>

### **ASCII**

<http://www.columbia.edu/kermit/ascii.html>

### **Authentication**

<http://www.e.govt.nz/services/authentication>

### **BPEL4WS**

<http://www-128.ibm.com/developerworks/library/specification/ws-bpel/>

### **CSV**

[http://www.answers.com/main/ntquery?method=4&dsid=1512&dekey=com+delimited&gwp=8&curtab=1512\\_1](http://www.answers.com/main/ntquery?method=4&dsid=1512&dekey=com+delimited&gwp=8&curtab=1512_1)

### **CVLs**

[http://en.wikipedia.org/wiki/Controlled\\_vocabulary](http://en.wikipedia.org/wiki/Controlled_vocabulary)

### **DNS**

<http://www.ietf.org/rfc/rfc1035.txt>

<http://www.cert.org/archive/pdf/dns.pdf> (DNS Security)

### **DocBook**

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=docbook](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=docbook)

### **DOM**

<http://www.w3.org/DOM/>

### **DRM**

<http://www.e.govt.nz/policy/trust-security/trust-security-2004/index.html>

(October 2004 paper on Trusted Computing)

### **DSML**

<http://www.oasis-open.org/specs/index.php#dsmlv2>

### **DTD**

<http://www.w3.org/TR/REC-html40/intro/sgmltut.html>

<http://www.w3schools.com/dtd/default.asp> (W3School's DTD Tutorial)

### **EbXML**

<http://www.ebxml.org/>

**ebXML MSG**

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=ebxml-msg](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-msg)

**ebXML RIM and RS V2.1 & v3.0**

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=regrep](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=regrep)

**ESA**

<http://www.linz.govt.nz/rcs/linz/pub/web/root/core/Topography/ProjectsAndProgrammes/emergencyservices/index.jsp>

**ESP**

<http://www.ietf.org/rfc/rfc2406.txt>

**FIPS 140-1 140-2**

<http://csrc.nist.gov/cryptval/140-1/1401val.htm>

<http://www.nist.gov/>

**FTP**

<http://www.ietf.org/rfc/rfc0959.txt>

<http://www.ietf.org/rfc/rfc2228.txt> (FTP security extensions)

<http://www.ietf.org/rfc/rfc1579.txt> (FTP via Port 80)

**G.711**

<http://en.wikipedia.org/wiki/G.711>

**G.729**

<http://en.wikipedia.org/wiki/G729>

**GCSB NZSITs**

<http://www.gcsb.govt.nz/publications/nzsit/index.html>

**GIF 89a**

<http://www.w3.org/Graphics/GIF/spec-gif89a.txt>

**GML**

<http://www.opengis.org/techno/implementation.htm>

**GZIP**

<http://www.gzip.org/>

**H.323 v2**

<http://en.wikipedia.org/wiki/H323>

<http://computing-dictionary.thefreedictionary.com/codec> (Codec)

**HL7**

**e-GIF Version 3.1**  
**PART 3 - RESOURCES**

<http://www.hl7.org/>

**HTML 4.01**

<http://www.w3.org/TR/html401/>

**HTTP 1.1**

<http://www.ietf.org/rfc/rfc2616.txt>

**HTTPS**

<http://www.ietf.org/rfc/rfc2818.txt>

**IPsec**

<http://www.ietf.org/rfc/rfc2402.txt>

<http://www.ietf.org/rfc/rfc2404.txt> (IP Security Authentication Header)

**IP v4**

<http://www.ietf.org/rfc/rfc0791.txt>

**IP v6**

<http://www.ietf.org/rfc/rfc2460.txt>

**JPG**

<http://www.ietf.org/rfc/rfc2435.txt>

**LDAP v3**

<http://www.ietf.org/rfc/rfc1777.txt>

**Metalogue**

<http://www.e.govt.nz/standards/nzgls/management/>

**MIME**

<http://www.ietf.org/rfc/rfc2049.txt>

**NTP 4.0**

<http://www.ntp.org/>

**NZGLS 2.0**

<http://www.e.govt.nz/standards/nzgls/standard>

**NZGLS Thesauri**

<http://www.e.govt.nz/standards/nzgls/thesauri>

**NZGMS**

<http://www.e.govt.nz/standards/e-gif/geospatial-information>



**New Zealand Government Web Standards and Recommendations v1.0**  
<http://www.e.govt.nz/standards/web-guidelines/web-standards-v1.0> replaces  
New Zealand Government Web Guidelines v2.1.

**OASIS DSS**

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=dss](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss)

**ODFOA 1.0**

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=office](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office)

**OIDS**

[http://en.wikipedia.org/wiki/Object\\_identifier](http://en.wikipedia.org/wiki/Object_identifier)

**OpenSAML**

<http://www.opensaml.org/>

**PDF**

<http://www.adobe.com/products/acrobat/adobepdf.html>

**PNG**

<http://www.libpng.org/pub/png/>

**Portal News Feed**

<http://www.e.govt.nz/standards/e-gif/rss>

**RDF**

<http://www.w3.org/RDF/>

**RSS**

<http://web.resource.org/rss/1.0/>

**RTP**

<http://www.ietf.org/rfc/rfc3550.txt>

**SAML**

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)

**SAX**

<http://www.w3.org/DOM/>  
[http://en.wikipedia.org/wiki/Simple\\_API\\_for\\_XML](http://en.wikipedia.org/wiki/Simple_API_for_XML)

**SCP**

<http://www.w3.org/Protocols/HTTP-NG/http-ng-scp.html>

**SDMX**

**e-GIF Version 3.1**  
**PART 3 - RESOURCES**

<http://www.sdmx.org/>

**SecureMail**

<http://www.e.govt.nz/services/securemail>

**SEEMail**

<http://www.e.govt.nz/services/see>

**SEE PKI**

<http://www.e.govt.nz/services/see> (SEE)

**Shared Workspace**

<http://www.e.govt.nz/services/workspace>

**S-HTTP**

<http://en.wikipedia.org/wiki/S-HTTP>

**SIGS**

<http://www.security.govt.nz/sigs/sigs.pdf>

<http://www.iso17799software.com/> (ISO 17799)

**SIP**

<http://www.ietf.org/rfc/rfc3261.txt>

<http://computing-dictionary.thefreedictionary.com/codec> (Codec)

**S/MIME v3.0**

<http://www.ietf.org/rfc/rfc2633.txt>

**SMTP**

<http://www.ietf.org/rfc/rfc2821.txt>

[http://www.cert.org/tech\\_tips/email\\_spoofing.html](http://www.cert.org/tech_tips/email_spoofing.html) (spoofing)

**SOAP 1.1**

<http://www.w3.org/TR/2000/NOTE-SOAP-20000508/>

**SOAP 1.2**

<http://www.w3.org/TR/2001/WD-soap12-20010709/>

**SSL v3**

<http://wp.netscape.com/eng/ssl3/ssl-toc.html>

**SVG**

<http://www.w3.org/Graphics/SVG/Overview.htm8>

**TAR**

<http://www.gnu.org/software/tar/tar.html>

**TCP**

<http://www.ietf.org/rfc/rfc793.txt>

**TLS**

<http://www.ietf.org/rfc/rfc2246.txt>

**Trusted Computing**

<http://www.e.govt.nz/policy/tc-and-drm/principles-policies-06/index.html>

(Principles and Policies)

<http://www.e.govt.nz/policy/trust-security/trust-security-2004/index.html>

(SSC Report 2004 on Trust and Security)

**UBL**

[http://www.oasis-open.org/committees/sc\\_home.php?wg\\_abbrev=ubl-ndrsc](http://www.oasis-open.org/committees/sc_home.php?wg_abbrev=ubl-ndrsc)

**UDDI**

<http://www.uddi.org/specification.html>

<http://www.w3.org/TR/2001/NOTE-wsdl-20010315> (WSDL)

**UDP**

<http://www.faqs.org/rfcs/rfc768.html>

<http://www.networksorcery.com/enp/protocol/udp.htm>

**UML**

<http://www.omg.org/technology/uml/index.htm>

**Unicode**

<http://www.unicode.org/>

**URN**

<http://www.e.govt.nz/standards/e-gif/urn-namespace>

<http://www.ietf.org/rfc/rfc4350.txt>

**UTC (MSL)**

<http://www.irl.cri.nz/msl/services/time/>

<http://www.unicode.org/> (Unicode Transformation Format)

**UTF – 8 bit encoded**

<http://www.ietf.org/rfc/rfc2279.txt>

**W3C schema definitions**

<http://www.w3.org/TR/xmlschema-1/>

**WebDAV**

<http://www.ietf.org/rfc/rfc2518.txt>

**WFS**

<http://www.opengeospatial.org/specs/>

**Win SCP**

<http://winscp.net/eng/index.php>

**Wireless standard**

<http://www.cnp-wireless.com/ArticleArchive/Wireless%20Telecom/2002Q3-SMSInterworking.htm> (Cellular Networking Perspectives LTD article on SMS interoperability)

**WMS**

<http://www.opengis.org/techno/implementation.htm>

**WordML**

<http://www.xmlw.ie/aboutxml/wordml.htm>

**WS-I Basic Profile 1.1**

<http://www.ws-i.org/profiles/BasicProfile-1.1-2004-08-24.html>

**WSS-I Basic Profile 1.0**

<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2004-05-12.html>

**WS – Security**

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=wss](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss)

**WSDL 1.1**

<http://www.w3.org/TR/2001/NOTE-wsdl-20010315>

**WSE2**

<http://www.microsoft.com/downloads/details.aspx?FamilyId=FC5F06C5-821F-41D3-A4FE-6C7B56423841&displaylang=en>

**xACML V2.0**

[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=xacml](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)

**xBRL**

<http://www.xbrl.org/Home/>

**xCIL**

<http://www.oasis-open.org/committees/ciq/ciq.html#7>

**Xcrl**

<http://www.oasis-open.org/committees/ciq/ciq.html#8>

**xForms**

<http://www.w3.org/TR/2003/REC-xforms-20031014/>

**XMI**

<http://www.omg.org/technology/documents/formal/xmi.htm>

**XML 1.0**

<http://www.w3.org/TR/REC-xml>

**XML 1.1**

<http://www.w3.org/TR/2002/WD-xml11-20020425/>

**XML-Dsig**

<http://www.w3.org/TR/2002/REC-xmlsig-core-20020212>

**XML encryption**

<http://www.w3.org/TR/xmlenc-core/>

**XMPP**

<http://www.ietf.org/rfc/rfc3920.txt>

**xNAL (nz) schema**

<http://www.e.govt.nz/standards/e-gif/xnal>

**xNALv2**

<http://www.oasis-open.org/committees/ciq/ciq.html#4>

**XSL**

<http://www.w3.org/Style/XSL/>

**XSLT**

<http://www.w3.org/Style/XSL/>

**ZIP 2.3**

<http://www.info-zip.org/>

## **2.7 e-GIF documents**

### **December 2001 New Zealand E-government Strategy**

<http://www.e.govt.nz/about-egovt/programme/e-gov-strategy-dec-01/>

### **June 2003 E-government Strategy Update**

<http://www.e.govt.nz/about-egovt/strategy/strategy-june-2003/>

### **November 2006 New Zealand E-government Strategy**

<http://www.e.govt.nz/about-egovt/strategy/nov-2006/>

### **Current version of the e-GIF**

<http://www.e-gif.govt.nz>

### **Frequently Asked Questions and Answers about the e-GIF**

<http://www.e.govt.nz/standards/e-gif/faqs.html>

## **2.8 Other New Zealand Government documents**

### **New Zealand Government Data Management Standards**

<http://www.e.govt.nz/standards/e-gif/data-management-standards>

### **New Zealand Government Data Management Policies**

<http://www.e.govt.nz/standards/e-gif/data-management-policies>

### **New Zealand Government Information Systems Policies and Standards**

<http://www.e.govt.nz/standards/e-gif/is-policies-standards>

### **New Zealand Government Web Standards and Recommendations v1.0**

<http://www.e.govt.nz/standards/web-guidelines/web-standards-v1.0> replaces  
New Zealand Government Web Guidelines v2.1 as of January 2007.

### **Guidelines for Managing and Monitoring Major IT Projects**

<http://www.ssc.govt.nz/ITguidelines>

### **Policy Framework for Government-held Information**

[http://www.ssc.govt.nz/documents/policy\\_framework\\_for\\_Government\\_.htm](http://www.ssc.govt.nz/documents/policy_framework_for_Government_.htm)

### **Privacy Act**

<http://www.privacy.org.nz/privacy-act/>

### **Security in the Government Sector**

<http://www.security.govt.nz/sigs/>

**Trusted Computing Principles and Policies**

<http://www.e.govt.nz/policy/tc-and-drm/principles-policies-06/index.html>

**SSC 2004 Report on Trust and Security**

<http://www.e.govt.nz/policy/trust-security/trust-security-2004/index.html>

**2.9 Other resources**

**Office of the UK e-Envoy**

<http://www.e-envoy.gov.uk/>

**UK Technical Standards Catalogue Version 6.2**

[http://www.govtalk.gov.uk/documents/TSCv6.2\\_2005\\_4\\_29.pdf](http://www.govtalk.gov.uk/documents/TSCv6.2_2005_4_29.pdf)

**Organization for the Advancement of Structured Information Standards (OASIS)**

<http://www.oasis-open.org/>

**International Organization for Standardization (ISO)**

<http://www.iso.org/>

**World Wide Web Consortium (W3C)**

<http://www.w3c.org/>

**Wikipedia (Definitions for protocols)**

[http://en.wikipedia.org/wiki/Protocol\\_%28computing%29](http://en.wikipedia.org/wiki/Protocol_%28computing%29)

[http://en.wikipedia.org/wiki/Communications\\_protocol](http://en.wikipedia.org/wiki/Communications_protocol)

**RFC 2119 (Key words for use in RFCs to indicate requirement levels)**

<http://www.faqs.org/rfcs/rfc2119.html>

### **3 Abbreviations**

The following abbreviations and acronyms are used in the e-GIF v3.1.

**ADL** Advanced Distributed Learning

**AS2** Applicability Statement 2

**ASCII** American Standard Code for Information Interchange

**B2B** Business-to-business

**BPEL4WS** Business Process Execution Language for Web Services

**CSV** Comma Separated Values

**CFL** Controlled Vocabulary or Code Lists

**DOM** Document Object Model

**DNS** Domain Name Server

**DSML** Directory Services Markup Language

**DSS** Digital Signature Services

**DTD** Document Type Definition

**EbXML (RIM, RS, MSG)** E-business XML (Registry Information Model, Registry Services, Messaging Services)

**EDI** Electronic data exchange

**ESA** Emergency Services in Government Administration

**ESP** IP Encapsulation Security Protocol

**FTP** File Transfer Protocol

**GCSB** Government Communications Security Bureau

**GIF** Graphical Interchange Format

**GML** Geography Markup Language

**HL7** Health Level 7



**HTML** HyperText Markup Language

**HTTP** HyperText Transfer Protocol

**HTTPS** HyperText Transfer Protocol running over SSL

**ICT Branch** Information and Communication Technologies Branch of the State Services Commission

**IMS** Instructional Management System

**IPsec** IP Security Authentication Header

**ITU-T** International Telecommunication Union – Telecommunication Standardization Sector

**LDAP** Lightweight Directory Access Protocol

**MIME** Multi-purpose Internet Mail Extensions

**NAT** Network Address Translation

**NTP** Network Time Protocol

**NZGLS** New Zealand Government Locator Service

**NZGMS** New Zealand Geospatial Metadata Standard

**NZSIT** New Zealand Security of Information Technology

**OASIS** Organization for the Advancement of Structured Information Standards

**ODFOA** Open Document Format for Office Applications (Open Document)

**OIDS** Schema Object Identifiers

**PKI** Public Key Infrastructure

**PNG** Portable Network Graphic

**RDF** Resource Description Framework

**RSS** Rich Site Summary

**RTP** Real-time Transport Protocol

**SAML** Security Assertion Markup Language

**SAX** Simple API for XML

**SCORM** Shareable Content Object Reference Model

**SCP** Session Control Protocol

**SDMX** Statistical Data and Metadata Exchange

**S.E.E.<sup>TM</sup> PKI** Secure Electronic Environment Public Key Infrastructure

**S-HTTP** Secure HTTP

**SIGS** Security in the Government Sector

**SIP** Session Initiation Protocol

**S/MIME** Secure Multi-purpose Internet Mail Extensions

**SMTP** Simple Mail Transfer Protocol

**SOAP** Simple Object Access Protocol

**SSH** Secure Shell

**SSL** Secure Sockets Layer

**SVG** Scalar Vector Graphics

**TCP/IP** Transmission Control Protocol / Internet Protocol

**TLS** Transport Layer Security

**TNEF** Transport Neutral Encapsulation Formats

**UBL** Universal Business Language

**UDDI** Universal Description, Discovery and Integration

**UDP** User Datagram Protocol

**UML** Unified Modelling Language

**URN** Uniform Resource Name

**UTC (MSL)** Universal Time Clock (Measurement Standards Laboratory)

**UTF** Unicode Transformation Format

**VPN** Virtual Private Network

**W3C** World Wide Web Consortium

**WebDAV** World Wide Web Distributed Authoring and Versioning

**WFS** Web Feature Server

**WMS** Web Map Server

**WSDL** Web Services Definition Language

**WS-I** Web Services-Interoperability Organisation

**xACML** Extensible Access Control Markup Language

**xBRL** Extensible Business Reporting Language

**xCIL** Extensible Customer Information Language

**xCRL** Extensible Customer Relationships Language

**XHTML** Extensible HyperText Markup Language

**XMI** XML Metadata Interchange

**XML** Extensible Markup Language

**XML-DSig** XML Digital Signatures

**XMPP** Extensible Messaging and Presence Protocol

**xNAL** Extensible Name and Address Language

**XSL** Extensible Stylesheet Language

**XSLT** Extensible Stylesheet Language Transformations