

STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga



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

Version 3.0

PART I – STANDARDS

September 2005

State Services Commission

About this document

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

- State Sector Information Technology (IT) strategists;
- Technical Analysts;
- Programme and Project Managers; and
- 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 statuses for each standard mean; links to related documentation; and changes from the last e-GIF;
- [E-GIF standards](#) – the standards, in table format, broken down by category; and
- [E-government services](#) – services that are part of the e-government programme, fully support interoperability, and are freely available to the agencies.

Table of Contents

1	How to read the standards	1
1.1	Layer model.....	1
1.2	Compliance status levels.....	3
1.3	Current e-GIF compliance statuses.....	4
1.4	Choosing between standards – agency considerations.....	6
1.5	Links.....	7
1.6	Comments.....	7
1.7	Changes from previous version.....	7
2	e-GIF standards	7
2.1	Network layer	8
2.1.1	Network Protocols (TCP/IP).....	8
2.1.2	Directory Protocols.....	8
2.1.3	File Transfer Protocols.....	8
2.1.4	Mail Transfer Protocols.....	9
	Registry Services.....	9
2.1.5	Time Protocols.....	9
2.1.6	Messaging Transport.....	10
2.1.7	Messaging Formats.....	10
2.2	Data Integration layer	10
2.2.1	Primary Character Set.....	10
2.2.2	Structured Web Document Language.....	10
2.2.3	Schema Definition Languages.....	11
2.2.4	Document Type Definition.....	11
2.2.5	Structured Data.....	11
2.2.6	Batch/bulk Data.....	11
2.2.7	File Compression.....	11
2.2.8	File Archiving.....	12
2.3	Business Services layer	12
2.3.1	Metadata (Discovery).....	12
2.3.2	Namespace.....	12
2.3.3	Schemas.....	13
2.3.4	Structured data description.....	13

2.3.5	Name and Address	13
2.3.6	Additional Customer Information	13
2.3.7	Customer Relationship	14
2.3.8	e-Learning	14
2.3.9	Business Reporting	14
2.3.10	Directory Services	14
2.3.11	Statistical Data and Metadata	14
2.3.12	Geospatial	15
2.3.13	Registry Services	15
2.3.14	Content Syndication and Channel Feeds	16
2.3.15	Instant Messaging	16
2.3.16	Voice Over Internet Protocol (VOIP)	16
2.4	Access and Presentation layer	17
2.4.1	Website Presentation	17
2.4.2	Web design and maintenance	17
2.4.3	Forms	17
2.4.4	Authentication Standards	17
2.5	Web Services layer	18
2.5.1	Discovery	18
2.5.2	Description	18
2.5.3	Access	19
2.5.4	Messaging	19
2.5.5	Security	19
2.5.6	Compliance	20
2.6	Security layer	20
2.6.1	Policy	21
2.6.2	Network	21
2.6.3	Data Integration	22
2.6.4	Web Services	22
2.6.5	Business Services	23
2.7	Best Practice layer	25
2.7.1	Digital Rights Management (DRM)	25
2.7.2	Trusted Computing	25
2.7.3	Process	25
2.7.4	XML Data Transformation	25
2.7.5	Data Modelling	26
2.7.6	Processing Structured Data	26
2.7.7	Controlled Vocabulary or code Lists (CVLs)	26
2.7.8	Health Sector	26
2.7.9	Document File Format	27
3	E-government services	27

1 How to read the standards

The e-GIF standards¹ are formatted in tables broken down using a “layer model”, structurally categorizing technology.

Each table includes protocols, standards and conventions (defacto standards), with version numbers where applicable, a status, review cycle, and 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 tables.

1.1 Layer model

Layer models are widely used to classify functions within IT systems. The intent is 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

¹ 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 and http://en.wikipedia.org/wiki/Communications_protocol.

The four basic structural components (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 Guidelines](#).

Applying to all of the structural layers are:

- **Security** – Crosses all layers, to reflect the fact it 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** – 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 made available by the ICT Branch for use by public-sector agencies. (See Part I, Section 3, E-government services)
- **Web Services** – An emerging set of standardised applications to connect and integrate web-based applications over the Internet. Web Services connect services together. Using Best Practice implementations, agencies can agree a common approach to interoperable service delivery to customers.

Underpinning all layers are:

- Management – See Part II, Managing the e-GIF.
- Governance – See Part II, Managing the e-GIF and Part II, Governance Principles. An e-GIF Governance overview paper is also available from the SSC ICT Branch. Please email e-GIF@ssc.govt.nz for access to this document.

1.2 Compliance status levels

The status level of an e-GIF standard indicates 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: Adopted, Recommended, Under Development, and Future Consideration. The revised statuses broadly align with the levels used in the UK e-GIF². The requirement for an additional category, Deprecated, became self 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, they give it an appropriate status. When the standard matures, the Committee can consider recommendations to alter its status.

² 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 statuses

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

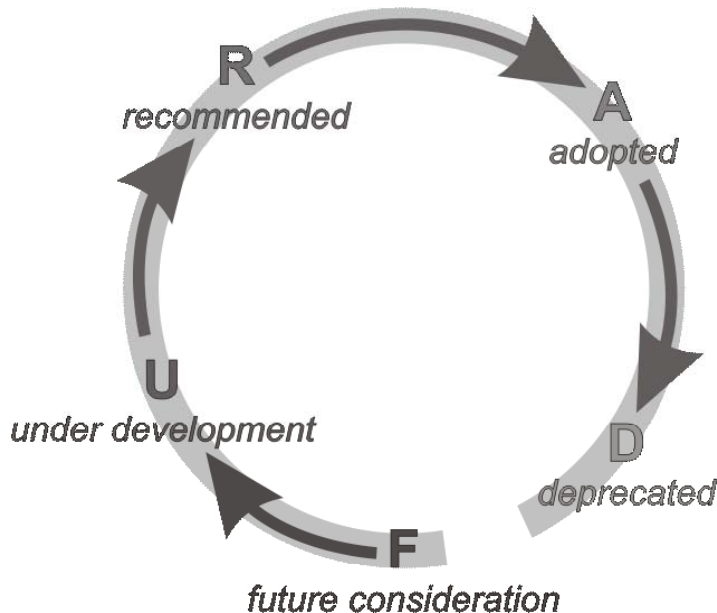


Figure 2: e-GIF Compliance Status Levels

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

- **Future Consideration (F):** – not yet reviewed, customised, nor having any successful, documented implementation in the New Zealand government; yet probably necessary for public-sector IT systems. Included mainly to introduce 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; and
 - not clashing with or rival to a standard already listed.
- **Under Development (U):** – actively under assessment by more than one government agency; for example, 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;
 - not clashing with or rival to a standard already listed; and
 - 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:
 - required for interoperability of IT systems in the public sector;
 - open;
 - scalable;
 - not overruled by an existing international standard;
 - not clashing with or rival to a standard already listed;
 - complete and published; and
 - showing clear indication of market support.
 - **Adopted (A)** – mandatory; 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:
 - 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; and
 - 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 twelve 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 in the Adopted or Recommended levels. Agencies should plan to migrate away from solutions assigned with this designation as soon as practical. New use of this standard is discouraged.

1.4 Choosing between standards – agency considerations

Given the need to maintain the e-GIF, to keep pace with changing technology, multiple standards may be available for an 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 with agencies whose functions and services relate to your own (your likely interoperability partners);
- then together agree a standard, considering the compliant statuses:
 - Use **R** (recommended) standards if you can; they are generally newer and less subject to obsolescence than **A** standards.
 - If you cannot or do not wish to use **R**, use **A** if you can (an **A** standard is the default; but if an **R** standard also exists, you are encouraged to use it).
 - If you cannot use **R** or **A** standards, use any applicable **F** or **U** standards and notify the SSC ICT Branch for Working Grouping 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 **D**.

Note that 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 that they will be participating 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 more fully explain them. If you are using a hard-copy version of this document, see Part III, *URLs Referenced In This Document*.

1.6 Comments

The comments column provides 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

The following elements of the standards tables are new to e-GIF version 3.0:

- **Statuses** – version 2.1 standards were either Mandatory or Recommended; this version uses the scheme described above.
- **Columns** – tables now include columns for Status, and Comments.
- **Web Services Section** – standards specifically related to Web Services implementation that do not strictly fit into the layer model.
- **Best Practice Section** – standards that do not strictly fit into the layer model but rather apply in a particular context only.
- **Added, moved, removed, revised standards** – see the *Change Log* in Part III.. Note that there are a number of new standards in version 3.0 of the e-GIF; many of were deemed 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. The abbreviations used in this section are spelt out at the end of the document. Links in the tables to online resources (usually the standards themselves) explain more fully what each covers; see also see Part III, *URLs Referenced In This Document*. For a list of standards that are new, moved, removed, or changed in this version, the *Change Log* in Part III.

Note that multiple standards may exist in any category (see “Choosing between standards – agency considerations”).

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 (TCP/IP)

Adopted protocols:

- [TCP](#) – Transmission Control Protocol.
- [UDP](#) – [User Datagram Protocol](#)
 - – A lower service level alternative to TCP, offers minimal transport service for applications using multicast/ broadcast delivery, DNS, routing information, and network management. Omission from previous version.
- [IP v4](#) – Internet Protocol Version 4
 - Plan for migration to IP v6. New hardware should support IP v4 as well as IP v6.

Recommended protocols:

- [IP v6](#) – Internet Protocol Version 6
 - When implementing IP v6, configure routers to “ghost” IP v4.

2.1.2 Directory Protocols

Recommended Protocol

Comments

- [LDAP v3](#) – Lightweight Directory Access Protocol Version 3
 - For access to directory services.

2.1.3 File Transfer Protocols

Adopted Protocol

- [FTP](#) – File Transfer Protocol
 - Use restart and recovery. Also [FTP security extensions](#) and [FTP via Port 80](#) where applicable.

- [HTTP v1.1](#) – HyperText Transfer Protocol Version 1.1
 - Application-level protocol. See [Security layer](#) for secure HTTP (HTTPS) and TLS usage.

Future Consideration

- [WebDAV](#) – World Wide Web Distributed Authoring and Versioning
 - 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
 - A simple protocol which lets a server and client have multiple conversations over a single TCP connection. The main function of SCP is to define a file transfer method that supports the transfer of files between a local and a remote computer. It uses Secure Shell (SSH) and supports Secure FTP.

2.1.4 Mail Transfer Protocols

Adopted Protocol

- [SMTP](#) – Simple Mail Transfer Protocol
 - Host-to-host protocol. Beware of [spoofing](#) of email addresses. SMTP-TLS is used to protect mail headers

Registry Services

Adopted Protocol

- [DNS](#) – Domain Name Server
 - Use DNS for Internet/Intranet domain to IP address resolution. [DNS Security](#) is critical. Omission from previous version.

2.1.5 Time Protocols

Under Development

- [NTP v4](#) – Network Time Protocol Version 4
 - De facto standard proposed for use in an all-of-government time standard. Best practice guidelines are being developed

Future Consideration

- [UTC \(MSL\)](#) – Universal Time Clock (Measurement Standards Laboratory)
 - De facto standard (accessed from Industrial Research Limited, MSL); proposed for use in an all-of-government time standard. Best practice guidelines are being developed

2.1.6 Messaging Transport

Adopted Protocol

- [HTTP v1.1](#) – HyperText Transfer Protocol Version 1.1
 - See [File Transfer](#) and [Security layer](#).

2.1.7 Messaging Formats

Adopted Protocol

- [MIME](#) - Multi-Purpose Internet Mail Extension
 - 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 the standards in the realm of data exchange and processes.

2.2.1 Primary Character Set

Adopted Component

- [ASCII](#) – American Standard Code for Information Exchange
 - Minimum set of characters for data interchange. Omission from previous version.
- [UTF – 8 bit encoded](#)
- [Unicode Transformation Fomat](#) – An extension of ASCII.

2.2.2 Structured Web Document Language

Adopted Protocol

- [HTML v4.01](#) – HyperText Markup Language Version 4.01
 - For web content.
 - See [Web Guidelines Version 2.1](#).

2.2.3 Schema Definition Languages

Adopted Protocol

- [XML v1.0](#) – Extensible Markup Language Version 1.0
 - Meta-language to create tags to define, transit, validate, and interpret data.

2.2.4 Document Type Definition

Adopted Protocol

- [DTD](#) – Document Type Definition
 - Describes multiple elements and attributes for XML; see [W3School's DTD Tutorial](#).

2.2.5 Structured Data

Adopted Protocol

- [XML v1.0](#) – Extensible Markup Language Version 1.0
 - Preferred option for structured data transport.

2.2.6 Batch/bulk Data

Deprecated Protocol

- [CSV](#) – Comma-Separated Values
 - XML 1.0 is strongly preferred for structured data transport. Parties must agree file header records before exchange. Omission from previous version.

2.2.7 File Compression

Adopted Protocol

- [ZIP v2.3](#) - ZIP Version 2.3
 - Other products using the compression algorithm LZH are also acceptable, subject to the agreement of the exchanging parties.

- [GZIP](#) – GNU Zip
 - Not compatible with ZIP. Omission from previous version.

2.2.8 File Archiving

Adopted Protocol

- [TAR](#) – Tape Archiver
 - Omission from previous version.

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)

Adopted Protocol

- [NZGLS v2.0](#) – New Zealand Government Locator Service Version 2.0
- [NZGLS Thesauri](#) – New Zealand Government Locator Service Thesauri
- [RDF](#) – Resource Description Framework
 - An XML file format to describe metadata. RDF is used by RSS1.0 (see later in this section).

2.3.2 Namespace

Adopted Protocol

- [W3C schema definitions](#) – World Wide Web Consortium Schema Definitions
 - Use when other schemas customised for use by government agencies are not specifically identified (e.g., NZGMS, xNAL (nz), NZGLS).

Recommended Protocol

- [OIDS](#) – Schema Object Identifiers
 - The State Services Commission (ICT Branch) maintains 2.16.544.101 as the Government OID Arc.

Under Development

- [URN](#)

- Uniform Resource Name – Working group to be led by SSC ICT Branch. See also [Internet Draft](#).

2.3.3 Schemas

Adopted Protocol

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

Adopted Protocol

- [XML v1.1](#) – Extensible Markup Language Version 1.1
 - Erratum in previous version. (Note: “Structured data” refers to XML Version 1.0.)

2.3.5 Name and Address

Adopted Protocol

- [xNAL v2](#) – Extensible Name and Address Language Version 2
 - xNAL (OASIS) Version 3 being drafted; will be incorporated into e-GIF following a successful pilot.

Recommended Protocol

- [xNAL \(nz\) schema](#) – Extensible Name and Address Language (New Zealand)
 - Agency User Group led by SSC ICTBranch; xNAL (nz) will ultimately be replaced by xNAL (OASIS) Version 3.

2.3.6 Additional Customer Information

Under Development

- Data formats for identity records standard
 - The All-of-government Authentication project is using 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.

Future Consideration

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

Future Consideration

- [xCRL](#) – Extensible Customer Relationships Language
 - Part of the xCIL and xNAL family of standards specifying formats for relationships between customers.

2.3.8 e-Learning

Future Consideration

- [ADL, SCORM, and IMS](#) – Advanced Distributed Learning, Shareable Content Object Reference Model, and Instructional Management System
 - Specifications currently being considered by the E-learning Working Group.

2.3.9 Business Reporting

Under Development

- [xBRL](#) – Extensible Business Reporting Language
 - Working Group underway, led by IRD.

2.3.10 Directory Services

Future Consideration

- [DSML](#) – Directory Services Markup Language.

2.3.11 Statistical Data and Metadata

Future Consideration

- [SDMX](#) – Statistical Data and Metadata Exchange
 - Statistics New Zealand leads this standard.

2.3.12 Geospatial

Adopted

- [GML](#) – Geography Markup Language
 - Land Information New Zealand leads this standard.
- [WFS](#) – Web Feature Server
 - Land Information New Zealand leads this standard.
- [WMS](#) – Web Map Server
 - Land Information New Zealand leads this standard.

Recommended

- [ESA](#) – Emergency Services in government Administration
 - Land Information New Zealand leads this standard.
- [NZGMS](#) – New Zealand Geospatial Metadata Standard
 - Schema for identifying geospatial metadata. Land Information New Zealand leads this standard.

2.3.13 Registry Services

Adopted Standards

- [ebXML RIM and RS v2.1](#) – E-business Extensible Markup Language, Registry Information Model, and Registry Services Version 2.1
 - – Open standard application for Registry Information and Records Services in an e-business context, as an alternative to Web Services.

Future Standards

- [ebXML RIM and RS v3.0](#) – E-business Extensible Markup Language, Registry Information Model, and Registry Services Version 3.0
 - 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

Recommended Standards

- [RSS](#) – Rich Site Summary
 - Note that this standard is required for agencies using the [government portal news service](#), [E-government Shared Services](#)).

2.3.15 Instant Messaging

Future Standards

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

2.3.16 Voice Over Internet Protocol (VOIP)

Future Standards

- [SIP](#) – Session Initiation Protocol
 - 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
 - Defines a standardized 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
 - An umbrella recommendation from the ITU-T, that defines the protocols to provide audio-visual communication sessions on any packet network. Taken from [UK Technical Standards Catalogue Version 6.2](#). [Codec](#) required.
- [G.711](#)
 - An ITU-T standard for audio companding; primarily used in telephony.
- [G.729](#)

- G.729 – An audio codec for voice that compresses voice audio in chunks of 10 milliseconds, and is mostly used in Voice over IP (VoIP) applications for its low bandwidth requirement.

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

Recommended Standards

- [NZ Govt Web Guidelines Version 2.1](#)
 - See Web Guidelines 2.1 for use of: HTML 4.01, XHTML, GIF 89a, JPG, PNG, SVG, and PDF.
 - Proposed change to Adopted status in 2006.

2.4.2 Web design and maintenance

Recommended Standards

- [NZ Govt Web Guidelines Version 2.1](#)
 - See Web Guidelines 2.1 for use of: HTML 4.01, XHTML, GIF 89a, JPG, PNG, SVG, and PDF.
 - Proposed change to Adopted status in 2006.

2.4.3 Forms

Future Standards

- [xForms](#)
 - Open standard for use of XML forms on web pages, to replace HTML forms.

2.4.4 Authentication Standards

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

Under Development

- Evidence of identity standard

- Specifies a business process for establishing the identity of government-agency customers.
- Username / passwords standard
 - Specifies use of username/passwords for online authentication.
- “Key type 2” standard
 - Specifies use of an as-yet-undefined key type for online authentication.
- Authentication key strengths standard
 - Specifies and populates a model for comparing the relative strengths of authentication keys.
- Trust levels for online transactions standard
 - Maps online transactions to authentication key strengths and evidence-of-identity confidence levels.

2.5 Web Services layer

Web services are 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 web-services implementation across government.

The following standards apply where systems use a web-services architecture.

2.5.1 Discovery

Adopted Standards

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

2.5.2 Description

Adopted Standards

- [WSDL v1.1](#) – Web Services Description Language Version 1.1

- Specifies the location of the service and the operations (or methods) the service exposes.

2.5.3 Access

Adopted Standards

- [SOAP v1.1](#) – Simple Object Access Protocol Version 1.1
 - For Web Services Transport. E-GIF v3.0 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.

Recommended Standards

- [SOAP v1.2](#) – Simple Object Access Protocol Version 1.2
 - Previous versions of e-GIF adopted SOAP v1.2. e-GIF v3.0 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

Future Consideration

- [ebXML MSG](#) – E-Business Extensible Markup Language Messaging Services
 - Also known as ebMS.
- [AS2](#) – Applicability Statement 2
 - A lightweight, open messaging transport for B2B messaging services. Comparable with ebXML MSG/ebMS.

2.5.5 Security

Future Consideration

- [WSS](#) – Web Services Security
 - Security standard under development by OASIS.
- [SAML v2.0](#) – Security Assertion Markup Language Version 2.0
 - 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
 - XML Schema for creating policies and automating their use to control access to disparate devices and applications on a network.

2.5.6 Compliance

Future Consideration

- [WS-I Basic Profile v1.1](#) - Web Services – Interoperability Organisation Basic Profile Version 1.1
 - Profiles provide implementation guidelines for how related web-services specifications should be used together for best interoperability. To date, WS-I has finalized 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
 - 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 it needs to be designed into a system, not added as a layer on top. Security can be viewed in four main contexts:

- **Confidentiality** – ensuring that information is accessible only to those authorised to have access
- **Integrity³** – safeguarding the accuracy and completeness of information and processing methods
- **Availability** – ensuring that authorised users have access to information and associated assets when required

³ 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.

- **Accountability** – the ability of a system to keep track of who or what has accessed data, conducted transactions, or made changes to the system⁴.

Agencies are encouraged to consider the Security implications of interoperability projects using these contexts, and apply the appropriate policies and standards. The following table 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.

2.6.1 Policy

Adopted Standard

- [GCSB NZSITs](#) – Government Communication Security Bureau New Zealand Security of Information Technology Publications
 - Please note that the NZSITs are currently being updated. Refer to GCSB for advice on hashing, key transport, signing, and cryptographic algorithms currently in the draft revision to the NZSIT400.
- [SIGS](#) – Security in the Government Sector
 - A manual of policies, principles and procedures mandated by Cabinet in 2001, largely drawn from [ISO 17799](#).
 - Page 8-20, paragraph 10 of SIGS requires use of an IS framework following ISO 17799 for all systems processing classified (including IN-CONFIDENCE) information or hosting government services.
 - Individual security counter-measures defined in ISO17799 should be considered, but are not mandated.

2.6.2 Network

Adopted Standard

- [HTTPS](#) - HyperText Transfer Protocol running over SSL
 - See SSL V3 below. Omission from previous version
- [SSL v3](#) - Secure Sockets Layer Version 3
 - Use for encrypted transmission of any data quantity between web browser and web server over TCP/IP. Uses HTTPS

⁴ Sourced from ISO17799: IT - Code of Practice for Information Security Management.

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

- [Ipssec - Internet Protocol Security](#)
 - Authentication Header standard taken from NZSIT/SIGS. Omission from previous version.
- [ESP - IP Encapsulation Security Protocol for VPN](#)
 - Requirements taken from NZSIT/SIGS. Omission from previous version.

Future Consideration

- [S-HTTP - Secure HyperText Transfer Protocol](#)
 - For individual messages, created by SSL running under HTTP.
- [TLS - Transport Layer Security](#)
 - 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

Future Consideration

- [XML - Enc](#) - XML-Encryption syntax and processing
 - Taken from [UK Technical Standards Catalogue Version 6.2](#).
- [XML-DSig](#) or [OASIS DSS](#)
 - 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

Future Consideration

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

- A subset of SAML V 1.1, elements are Under Development as part of the All-of-government Authentication project. See [Access and Presentation layer](#).

Under Development

- Security Assertion Messaging standard
 - 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

Recommended Standard

- [SEE PKI](#) - Secure Electronic Environment Public Key Infrastructure
 - For agencies using the [Secure Electronic Environment](#) (SEE) e-government component. See [E-government services](#) for more details.
- [SEEMail](#) - Secure Electronic Environment Mail
 - A combination of procedures and standards already listed in the e-GIF, required to use the e-government component SEEMail service. See [E-government services](#) for more details.

Adopted Standard

- [S/MIME v3 0](#) - Secure Multi-Purpose Internet Mail Extensions Version 3
 - – Use MIME when security is not a concern. Use S/MIME encryption when not using the Messaging Transport protocols.

Under Development

- [SecureMail](#)

- A combination of procedures and standards already listed in the e-GIF required to use the e-government component SEEMail service. See [E-government services](#) for more details.

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)

Under Development

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

Under Development

Discussion paper on [Trust and Security on the Internet](#)

No convention yet – see [EGU Report on Trust & Security](#). A Working Group is considering conventions for use across government.

2.7.3 Process

Adopted Standard

- [BPEL4WS](#) – Business Process Execution Language for Web Services
 - Lets users describe business-process activities as Web services and define how they can be connected to accomplish specific tasks. Omission from previous version.

2.7.4 XML Data Transformation

Adopted Standard

- [XSLT](#) - eXtensible Stylesheet Language Transformations
 - A description vocabulary used by XSL to describe how an XML document is transformed into another XML document.

2.7.5 Data Modelling

Adopted Standard

- [UML](#) - Unified Modelling Language
 - Useful for describing objects in a visual format.

Recommended Standard

- [XMI](#) - XML Metadata Interchange
 - Enables easy interchange of metadata between modelling tools such as UML and remote metadata repositories.

Future Consideration

- [UBL](#) - Universal Business Language
 - Naming and design rules for schema design.

2.7.6 Processing Structured Data

Adopted Standard

- [SAX](#) - Simple API for XML
 - Parser for large volume repetitious batch transfers. Open standard for navigating and updating XML documents.

Recommended Standard

- [DOM](#) - Document Object Model
 - Parser for transactional exchanges. SAX is a Java API for navigating XML documents.

2.7.7 Controlled Vocabulary or code Lists (CVLs)

Future Consideration

- Discussion on [standardising CVLs](#).
 - Research underway, led by SSC ICT Branch.

2.7.8 Health Sector

Under Development

- [HL7](#) - Health Level 7

- An international standard adopted by the Health sector. Are converging on HL7 Version 2.4 for laboratory results and National Health Index (NHI).

2.7.9 Document File Format

Future Consideration

- [ODFOA v1.0](#), [DocBook](#), [WordML](#) - Open Document Format for Office Applications Version 1.0, DocBook, Word saved as XML
 - Several candidates for agencies to save documents in an open, XML format. The Parliamentary Counsel Office's [PAL project](#) leads this initiative.

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 government 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 web sites.
- **Authentication** - [Government to Individual and Government to Business online authentication](#)
 - This project is in Phase 1, referred to as the Shared Logon Initial Implementation. This phase is developing and trialling a Government (also known as Shared/Common) Logon Service to help agencies authenticate New Zealanders wishing to access agency services. Agencies interested in joining the trial should contact the [SSC ICT Branch](#).
- **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.
- **Government Intranet** - All-of-Government Online information repository
 - This is currently in pilot with a limited number of agencies before roll-out later in 2005.
- **SEE Mail and SecureMail** - New Zealand Secure Email Requirements; [SEE Mail](#) and [SecureMail](#)
 - Secure email. Two domains are offered:
 - SEE Mail is a gateway-gateway crypto layer running over public email, improving confidentiality and authentication. Intended for use between government bodies (including local government). Note that the next version of this service will not accept UUENCODE or TNEF message formats.
 - SecureMail is an extension of SEEMail to allow the use of secure email by the New Zealand public.

Please note that government agency web search capability is under review. Agencies considering products are advised to contact the SSC ICT Branch.