

STATE SERVICES COMMISSION
Te Kōmihana O Ngā Tari Kāwanatanga



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

Version 3.3

PART 1 – STANDARDS

February 2008

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

New Zealand E-government	i
Interoperability Framework	i
(NZ e-GIF)	i
Version 3.3	i
PART 1 – STANDARDS	i
February 2008	i
1 How to read the standards	1
1.1 Layer model	1
1.2 Compliance status levels	3
1.3 Current e-GIF compliance status levels	4
1.4 Choosing between standards	6
1.5 Links	6
1.6 Comments	7
1.7 Changes from previous version	7
2 e-GIF standards	8
2.1 Network layer	8
2.1.1 Network protocols.....	8
2.1.2 Directory protocols.....	8
2.1.3 File transfer protocols.....	8
2.1.4 Mail transfer protocols.....	9
2.1.5 Registry services.....	9
2.1.6 Time protocols.....	10
2.1.7 Messaging transport.....	10
2.1.8 Messaging formats.....	10
2.1.9 Digital Radio Communications.....	10

2.2 Data Integration layer	11
2.2.1 Primary character set	11
2.2.2 Structured web document language	11
2.2.3 Schema definition languages	11
2.2.4 Document type definition	12
2.2.5 Structured data	12
2.2.6 Batch/bulk data	12
2.2.7 File compression	12
2.2.8 File archiving	12
2.3 Business Services layer	13
2.3.1 Metadata (Discovery)	13
2.3.2 Namespace	13
2.3.3 Schemas	14
2.3.4 Structured data description	14
2.3.5 Name and address	14
2.3.6 Additional customer information	14
2.3.7 Customer relationship	15
2.3.8 E-learning	15
2.3.9 Business reporting	15
2.3.10 Directory services	15
2.3.11 Statistical data and metadata	16
2.3.12 Geospatial	16
2.3.13 Registry services	17
2.3.14 Content syndication and channel feeds	17
2.3.15 Instant messaging	17
2.3.16 Voice Over Internet Protocol (VOIP)	18
2.3.17 Digitisation	18
2.4 Access and Presentation layer	19
2.4.1 Website presentation	19
2.4.2 Web design and maintenance	19
2.4.3 Forms	19
2.4.4 Authentication standards	19
2.5 Web Services layer	21
2.5.1 Discovery	21
2.5.2 Description	21
2.5.3 Access	21
2.5.4 Messaging	22
2.5.5 Security	22
2.5.6 Compliance	23
2.6 Security layer	23
2.6.1 Policy	24
2.6.2 Network	25

2.6.3	Data integration.....	26
2.6.4	Web services	26
2.6.5	Business services	26
2.6.6	Public Key Infrastructure (PKI).....	27
2.7	Best Practice layer	28
2.7.1	Digital Rights Management (DRM).....	28
2.7.2	Trusted computing	28
2.7.3	Process	28
2.7.4	XML data transformation.....	29
2.7.5	Data modelling	29
2.7.6	Processing structured data	29
2.7.7	Controlled Vocabulary or code Lists (CVLs)	30
2.7.8	Health sector	30
2.7.9	Document file format.....	30
2.7.10	Biometrics	31
2.7.11	Evidence collection	31
2.7.12	Business Transactions	31
3	E-government Services	32

1 How to read the standards

The e-GIF standards¹ 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 v3.3 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, 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-focused 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.

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-GIF². 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.

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 status levels

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

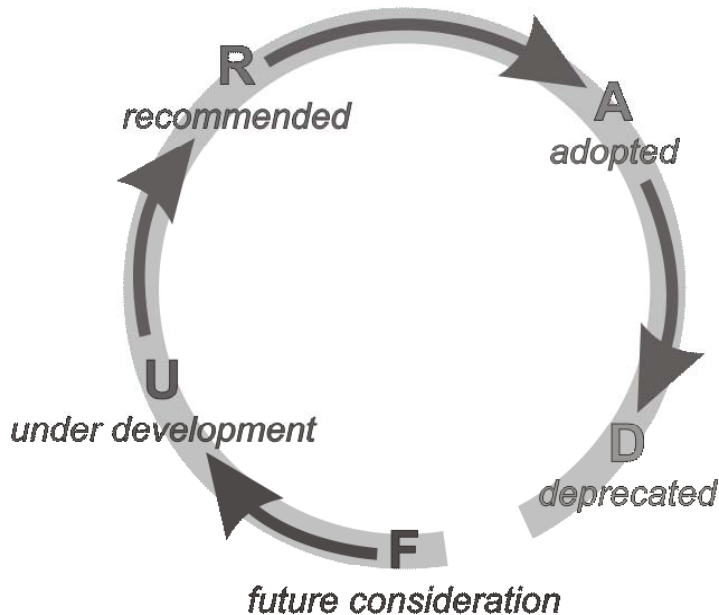


Figure 2: e-GIF Compliance Status Levels

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

- 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:

- **Messaging Formats section:** Section 2.1.8 added SOAPv1.2
- **Network Layer section:** Section 2.1.9 added APCO-P25
- **Schemas section:** Section 2.3.3 updates to UMCLVV
- **Name and Address section:** Section 2.3.5 updates to xNAL v2 and xNAL (nz)
- **Geospatial Information section:** Section 2.3.12 added WCS, updated ESA and NZGMS
- **Content Syndication section:** Section 2.3.14 added GeorSS
- **Web Services section:** Section 2.5.6 updated references to WS-I and WSS-I.
- **Best Practice section:** Section 2.7.10 updated comments on Biometrics.

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

IP v4 **Internet Protocol Version 4**
Status Adopted
Comments Plan for migration to IP v6. New hardware should support IP v4 as well as IP v6.

IP v6 **Internet Protocol Version 6**
Status Recommended
Comments When implementing IP v6, configure routers to “ghost” IP v4.

2.1.2 Directory protocols

LDAP v3 **Lightweight Directory Access Protocol Version 3**
Status Recommended
Comments For access to directory services.

2.1.3 File transfer protocols

FTP **File Transfer Protocol**
Status 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.

SOAP v1.2 **Simple Object Access Protocol**
Status Recommended
Comments Lightweight protocol intended for exchanging structured information in a decentralised, distributed environment.

2.1.9 Digital Radio Communications

APCO-P25 **APCO Project 25**
Status Adopted

- Common Air Interface (CAI)
- Analogue FM transceivers
- Digital P25 Phase 1 transceivers

Status Future consideration

- CAI for FDMA trunked digital systems

- Inter subsystem interface (ISSI)
- Fixed station interface
- Data peripheral interface
- Fixed host data interface
- PSTN interface
- Console subsystem interface

Comments Project 25 (P25) or APCO-25 refer to a suite of standards for digital radio communications for use by public safety agencies to enable them to communicate with other agencies and mutual aid response teams in emergencies. In this regard, P25 fills the same role as the European Tetra protocol (see <http://www.tetramou.com/tetramou.aspx?id=39>), although not interoperable with it.

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

<u>DTD</u>	Document Type Definition
Status	Adopted
Comments	Describes multiple elements and attributes for XML; see W3School's DTD Tutorial .

2.2.5 Structured data

<u>XML v1.0</u>	Extensible Markup Language Version 1.0
Status	Adopted
Comments	Preferred option for structured data transport.

2.2.6 Batch/bulk data

<u>XML</u>	Extensible Markup Language
Status	Adopted
Comments	XML 1.0 is preferred for structured data transport. Parties must agree file header records before exchange.

<u>CSV</u>	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

<u>ZIP v2.3</u>	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.

<u>GZIP</u>	GNU Zip
Status	Adopted
Comments	Not compatible with ZIP.

2.2.8 File archiving

<u>TAR</u>	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).

[UBL](#) Universal Business Language

Status Future Consideration
Comments Naming and design rules for schema design.

[UMCLVV \(for CVLs\)](#) UBL Methodology for Code List and Value Validation

Status Future Consideration
Comments Used for contextual validation in XML instances of sets of coded values expressed outside of the instances.

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 as part of OASIS CIQ 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 as part of OASIS CIQ 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 Deprecated

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 Under Development

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 Information

GML **Geography Markup Language**

Status Adopted

Comments Land Information New Zealand leads this standard.

WFS **Web Feature Service**

Status Adopted

Comments Land Information New Zealand leads this standard with the working group, Open Geospatial Consortium International.

WMS **Web Map Service**

Status Adopted

Comments Land Information New Zealand leads this standard with the working group, Open Geospatial Consortium International.

NZGMS **New Zealand Government Geospatial Metadata Standard**

Status Adopted

Comments Land Information New Zealand leads this standard. See also: <http://www.linz.govt.nz/resources/geospatial/xml/schema/nzgm-profile-pt1v1.2.pdf>

ESA **Emergency Services and Government Administration Core Data Specification**

Status Recommended

Comments Land Information New Zealand leads this standard. The most current version is V1.9.7 published in 2004. See also <http://www.linz.govt.nz/core/topography/projectsandprogrammes/emergencyservices/index.html>.

WCS **Web Coverage Service 1.1.0**

Status Future Consideration

Comments Open Geospatial Consortium (OGC)

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.

[ATOM 1.0](#) Syndication Format

Status Future Consideration

Comments XML-based syndication format. Development was motivated by the existence of many incompatible versions of the RSS syndication format. [Wikipedia](#) has a comparison of ATOM 1.0 with RSS 1.0.

[GeoRSS](#) Geospatial Resource Syndication Service

Status Future Consideration

Comments Geographically Encoded Objects for RSS feeds

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 Standards 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 1.2](#) 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 v3.3 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 v3.3 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.

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 v1.2](#) Web Services – Interoperability Organisation Basic Profile Version 1.2.

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. The Authentication Standards Secure Messaging Working Group will develop a 'secure messaging over web services' profile from the WS-i profiles during 2008.

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

Status Future Consideration

Comments Draft 1.1 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.

- **Integrity³**: 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 system⁴.

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.

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.

4 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 Recommended

Comments Digital rights management (DRM) is a set of technologies designed to apply and enforce persistent access restrictions to digital information, as specified by the information provider.

2.7.2 **[Trusted computing](#)**

Status Recommended

Comments Trusted computing is a combination of software and hardware supporting applications to ensure that data cannot be accessed unless the user's system is operating as expected and has not been tampered with. 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.

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 language used by [XSL](#) for transforming XML documents into other XML documents.

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.

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).

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](#)
 - Due for decommissioning in March 2008
 - A web-based repository for metadata, used to drive the government Portal <http://newzealand.govt.nz>.
- **Portal News Feed:** [News Syndication](#)
 - Due for decommissioning in March 2008
 - Uses NZ Government RSS to accept news items from government agencies for display on the government 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>.
- **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.

- **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>.