Technical Standard [TS04/18]

Common Alerting Protocol CAP-NZ

Common Alerting Protocol: CAP-NZ

Technical Standard [04/18]

February 2018
ISBN 978-0-478-43520-7
Published by the Ministry of Civil Defence & Emergency Management

Authority

This technical standard has been issued by the Director of the Ministry of Civil Defence & Emergency Management pursuant to s9(3) of the Civil Defence Emergency Management (CDEM) Act 2002.

This document is available, along with further information about the Ministry, on the MCDEM website www.civildefence.govt.nz.

Ministry of Civil Defence & Emergency Management
PO Box 5010
Wellington 6145
New Zealand
Tel: +64 4 817 8555
Fax: +64 4 817 8554

Email: emergency.management@dpmc.govt.nz
Website: www.civildefence.govt.nz

Foreword

In today's highly technical environment, emergency alerts may be sent and received through many media, such as websites, SMS, smartphone apps and roadside signs, in addition to the more traditional channels of radio and television.

Common Alerting Protocol (CAP) is a digital format for exchanging emergency alerts. It supports effective warnings by ensuring message consistency and enabling simultaneous distribution over many communication channels.

The New Zealand CAP Working Group was established in 2015 to coordinate and support the development of guidelines for the use of CAP in New Zealand. This technical standard for the emergency management sector is the outcome of that work.

The primary audience for this standard is New Zealand's official alerting authorities, their technology providers, and any suppliers developing or implementing public alerting mechanisms in New Zealand.

I am pleased to offer this standard to drive the continued uptake of CAP in New Zealand, leading to efficient and consistent warnings, and ensuring we have safer and more informed communities.

Sarah Stuart-Black

Director of Civil Defence Emergency Management

Contents

Section 1 Introduction

Common Alerting Protocol (CAP) is an international XML[1]-based open, non-proprietary digital message format for exchanging all-hazard emergency alerts. It supports consistency in the application of public warnings across Alerting Authorities, and the dissemination of warnings over many channels at the same time. The net result is increased effectiveness of warnings.

This document represents the current collection of specifications and recommended practices related to the standardisation of public alerts in New Zealand using the CAP standard. It has received input from all official New Zealand Alerting Authorities, other associated organisations and some commercial alerting hardware providers.

The CAP standard[2] was developed by the Organisation for the Advancement of Structured Information Standards (OASIS) and is based on best practices identified in academic research and practical experience. The International Telecommunication Union, Telecommunication Standardization Sector (ITU-T) adopted CAP in 2007. This technical standard should be used in conjunction with the Common Alerting Protocol V1.2 Practices Guide Version 2.0[3], which contains a wide range of practical advice based on the experiences of CAP implementation internationally.

Adopting and using CAP-enabled systems in New Zealand will enhance warning capability by providing one format for all warnings, no matter what the warnings are for. It also facilitates consistent behaviour of computer systems and message output channels across all warnings. CAP provides the capability to include 'rich data content', such as maps, photographs, streaming audio and video, as well as having the ability to target warnings to a defined area, and give different types of priority to warnings.

1.1 Purpose

The purpose of this document is to provide a guideline for the implementation of CAP in a New Zealand alerting context (CAP-NZ). It aims to provide clarity for Alerting Authorities on the formatting and categorisation of alerts, and how those alerts should then reach the public via public alerting dissemination systems and technologies.

1.2 Scope

This technical standard supports official New Zealand Alerting Authorities to originate and disseminate their alerts in CAP format, including:

- standardisation guidelines
- the role of CAP Hubs
- an explanation of the links to the World Meteorological Organization (WMO) Register of Alerting Authorities, and the OASIS CAP Standard.

[1] Extensible Mark-up Language (XML) is a document-annotating language that defines a set of rules for encoding documents in a format which is both human and machine readable.

[2] http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

[3] https://www.oasis-open.org/committees/document.php?document_id=59021&wg_abbrev=emergency-cap

This technical standard does not cover:

- instructions for the media on how to pass on warnings to the public
- the wider context for consistent messages, i.e. previously-agreed words with a clear meaning in an alerting context.

1.3 Audience

This technical standard is written for:

- Alerting Authorities originating or disseminating a public alert in New Zealand
- Alerting Authorities' technology providers
- any organisation (including technology vendors and industry) developing or implementing public alerting dissemination mechanisms for New Zealand.

1.4 Context

In New Zealand, warnings are issued by the agency that, through its normal line functional responsibilities, is involved with the identification and analysis of particular hazards and threats. These warnings are disseminated to other government agencies, relevant local organisations, corporate institutions, media, and in some cases directly to the public. For illustration, potential emergency situations and current public alerting responsibilities are included in Table 1.

Table 1 - Examples of threats and alerting agencies

Threat	Responsible Alerting Agency
Bio-security incursion	Ministry for Primary Industries
Criminal activity	New Zealand Police
Dangerous structure	New Zealand Police, local authorities
Earthquake notification	GNS Science
Fast moving fires	Fire and Emergency New Zealand
Flooding	Local authorities
Food safety threat	Ministry for Primary Industries
Hazardous chemical incident	Fire and Emergency New Zealand
Public health threat	Ministry of Health
Severe weather	MetService
Tsunami	Ministry of Civil Defence & Emergency Management (MCDEM), local authorities
Utilities failure	MCDEM, local authorities, lifeline utility providers
Volcanic activity	GNS Science

A survey conducted in 2014[4] identified about 20 existing public alerting options used by the civil defence emergency management sector alone, ranging from smartphone apps, email, websites, billboards, mobile loud speakers, fixed sirens, and several others.

[4] http://shop.gns.cri.nz/sr_2014-066-pdf/

Section 2 Governance

A CAP-NZ Governance Committee was established by the Hazard Risk Board, one of the governance boards of Officials' Committee for Domestic and External Security Coordination. The Committee consists of senior officials responsible for public alerting, and is also advised by the Government Chief Digital Officer, who facilitates links to Standards New Zealand at the Ministry of Business, Innovation and Employment. In October 2017, the CAP-NZ Governance Committee was incorporated into the Public Alerting Governance Committee.

The New Zealand CAP Working Group is chaired by the Ministry of Civil Defence & Emergency Management. It does not have any decision-making capacity; instead it makes recommendations to the Public Alerting Governance Committee.

The Public Alerting Governance Committee considers and approves the specification documents that comprise CAP-NZ, as advised by the CAP-NZ Working Group. It is also responsible for change management.

The Government Chief Digital Officer manages the technical component of CAP-NZ through the Government Enterprise Architecture Group, reporting through the ICT Partnership Framework, and advising the Public Alerting Governance Committee on technical matters.

The Hazard Risk Board signs off the ***CAP-NZ*** technical standard, with endorsement from the Chair of Officials' Committee for Domestic and External Security Coordination.

2.1 Business owner

MCDEM is the business owner for the CAP-NZ technical standard. For questions or comments on this technical standard, contact MCDEM by emailing emergency.management@dpmc.govt.nz.

2.2 Review of this technical standard

This technical standard will be reviewed by the CAP-NZ Working Group annually. Formal approval of the changes will be sought from the Public Alerting Governance Committee and included in its annual report to the Hazard Risk Board.

Urgent corrections may be advised to the Business Owner at any time and will be published in draft form until formal approval has been granted.

2.3 Registration as an alerting authority

Each Alerting Authority using CAP in New Zealand must be registered as such. Official New Zealand Alerting Authorities must uniquely identify themselves via their internationally unique *Object Identifier* (see Appendix B Registration as an Alerting Authority on page 21) in CAP messages in the <identifier> element.

Appendix B describes the criteria and process for registering Alerting Authorities.

Section 3 Origination, hubs and redistribution

Origination of CAP messages may be via automated systems implemented by an Alerting Authority, or by a manual process that an Authority has access to – for example, a web portal to create alerts. This message is automatically placed on an internet news feed.

CAP Hubs scrape[5] these feeds, and aggregate CAP messages from a number of Alerting Authorities. Alerting systems monitor the CAP Hubs for alerts that apply to their particular areas of responsibility, and send applicable alerts to the public. A number of global organisations operate such hubs, such as Google Public Alerts[6] and the Federation for Internet Alerts[7].

Once an internet news feed is available, anyone can take a CAP message from that feed and read it and redistribute it, including publishing it. Ideally it will be redistributed according to any audience-specific parameters, attributed to the originator, timestamped and updated, in a timely manner, and will be seen by the audience unmodified. However, the originator has no explicit control over this happening correctly.

For non-public communications, some control is available through the use of restricted lists for CAP messages intended for specific audiences (public or non-public), see section 5.1.6 <scope> - mandatory element, <restriction> conditional element and <addresses> - conditional element on page 11. Note that flagging a message as restricted is not a guaranteed control.

3.1 Verifying an alert is from an Alerting Authority

All CAP messages must list the originating agency in the <senderName> element. The Alerting Authority Object Identifier should also be included in the <identifier> element. This allows for alerts to be verified by alert redistributors against the World Meteorological Organization Register of Alerting Authorities. However, there is no guarantee that the message was actually originated by that agency, beyond the known nature of the internet news feed or CAP Hub on which it has been found. Therefore, CAP messages should be digitally signed by the originator. This ensures receivers of the message can be sure of the authenticity of the sender and that it has not been modified after it was issued. Alert redistributors or receiving systems can automatically check the signature for this formal verification.

3.2 Validating the CAP message

For the purposes of rigorous development and testing of new origination platforms, CAP messages must be validated by the originator when designing the XML layout, for example when writing automated code, or designing a form. Google have an online validator at https://cap-validator.appspot.com/. This is a free service that checks the syntax of CAP XML messages and supports Atom, RSS and EDXL[8] feeds of CAP messages. Google has additional recommendations[9] for use of the CAP format. We recommend following these to allow for Google redistribution of New Zealand CAP messages.

[5] *Scrape* means to continuously monitor the feed and take up new content when it is published.

[6] https://alert-hub.appspot.com/

[7] https://www.internetalerts.org/hub/dashboard

[8] Atom, RSS and EDXL are standard formats for internet news feeds.

[9] https://developers.google.com/public-alerts/?visit_id=0-636515580461668407-97895553&rd=1

It is the responsibility of the originating agency to issue valid CAP messages. It is also the responsibility of any receiving or re-originating agency to ensure any CAP messages they receive are valid.

3.3 Validating the CAP feed

A Google tool at https://cap-validator.appspot.com/subscribe will monitor CAP feeds and messages, and email any exception alerts. The majority of these are time-out alerts rather than malformed CAP messages.

3.4 Re-origination of a modified alert

The public should not get several similar alerts in a short period of time (i.e. a few minutes) – they may ignore new messages, or miss the important additions in the messages. However, if two alerts are significantly different, for example details about an event compared to detailed instructions, they may arrive close together in time.

Whenever an Alerting Authority wants to modify or add to a CAP message, it must be re-originated.

Section 4 Defining the strength of an alert

Three elements are at the core of CAP: *urgency*, *severity* and *certainty*. They define the overall strength of an alert by its imminence, impact and likelihood. The possible values for the levels of each are shown in Table 2.

Table 2 - Levels of Urgency, Severity and Certainty

Level	Description
Urgency:	
Immediate	Responsive action *should* be taken immediately
Expected	Responsive action *should* be taken soon (within next hour)
Future	Responsive action *should* be taken in the near future
Past	Responsive action is no longer required
Severity:	
Extreme	Extraordinary threat to life or property
Severe	Significant threat to life or property
Moderate	Possible threat to life or property
Minor	Minimal to no known threat to life or property
Certainty:	
Observed	Determined to have occurred or to be ongoing
Likely	Likely (p > approximately 50%)
Possible	Possible but not likely ($p \leq$ approximately 50%)
Unlikely	Not expected to occur ($p \sim 0$)
Although a possible value, **Unknown** *should not be used for any of these three elements.* **Unknown** *is not equivalent to minimal.*	

4.1 Further guidance

***Urgency*:** Choosing the level of Urgency should also include any time for action - the minimum amount of time people could reasonably be expected to carry out the instructions in the alert. For example:

- **5 minutes**: 'Do not take personal belongings other than critical medication and personal documents'
- **30 minutes**: 'Bring in outdoor objects such as lawn furniture, toys and garden tools, and anchor objects that cannot be brought inside'

Severity: *Extraordinary threat* applies to an emergency affecting a town, city or a region:

- **Life**: widespread deaths are possible; or
- **Health**: widespread permanently incapacitating injuries or illness are possible; or
- **Property**: widespread destruction (or rendering uninhabitable) of buildings is possible

Significant threat applies to an emergency affecting rural dwellers, or a small part of a suburb in an urban area:

- **Life**: limited deaths (i.e. individuals or small groups) are possible; or
- **Health**: limited permanently incapacitating injuries or illness are possible; or
- **Property**: limited (i.e. few or very localised) destruction (or rendering uninhabitable) of buildings is possible

***Certainty*:** **Likely** should consider that a qualitative estimate of probability may vary by up to 30%, and erring on the side of caution may be preferable in some circumstances. The desire to wait for certainty is a trade-off against allowing sufficient time for action.

4.2 High-priority alerts

Alerts with the highest level of importance are called *High-priority alerts*. CAP-NZ conforms to the emerging global standard threshold, which states that High-priority alerts are defined to be at the following levels of urgency, severity and certainty:

1. Urgency: *Immediate* or *Expected*
2. Severity: *Extreme* or *Severe*
3. Certainty: *Observed* or *Likely*

Section 5 CAP-NZ element content and guidance for use

This section lists New Zealand-specific guidance for the content and use of each CAP-specified standard XML element that is required or recommended for New Zealand. It should be read in conjunction with the OASIS CAP standard and the Google Public Alerts Technical Guide[10] ("Elements Definitions").

Elements are marked by an opening and closing tag, each tag enclosed in < > characters as is usual with XML. Technically the element name does not include the < > characters, but elements are presented throughout this technical standard with those characters for ease of identification. Elements are:

Table 3 - CAP content elements that this technical standard requires (shown in bold) or recommends (shown in italics)

Element name	Purpose
<alert>	
<identifier>	Alerting Authority identification (including Object Identifier).
<sender>	Web address of the sender.
<sent>	Time alert was originated.
<status>	Message status.
<msgType>	Message type.
<scope>, <restriction> and <addresses>	Management of message distribution.
<area>	
<areaDesc>, <polygon>, <circle> and <geocode>	Used for geo-targeting alerts.
<info>	
<category>	Event category.
<event>	Descriptive term for nature of event, e.g. Tsunami, Storm Surge, Tropical Cyclone.
<eventCode>	Standard label for hazard and warning event types, see Appendix C for the current list used in New Zealand.
<urgency>, **<severity>** and **<certainty>**	Together these elements define the strength of the alert.
<effective>	Effective start time for the alert.
<expires> and *<responseType>*	Expiration time of the alert and "All Clear".
<senderName>	The Alerting Authority's identification – the organisation's full name.
<headline>	At a minimum, the <headline> element should contain all key messages, for receiving systems that do not carry more than 140 characters such as SMS.

[10] https://docs.google.com/document/pub?id=1J7bz05S6C1c5WvCd4m6f9asGoKqUpa2OUsaqx4SPKzM

Element name	Purpose
<*description*>, <*instruction*>	Every CAP alert should include content in a 'what happened' / 'is expected to happen' <description> element and a 'call to action' <instruction> element. The <instruction> and <description> text must not be the same.
<language>	The language of the <info> element.

Figure 1 below is reproduced from the OASIS CAP standard, and includes many of the standard CAP elements, for reference.

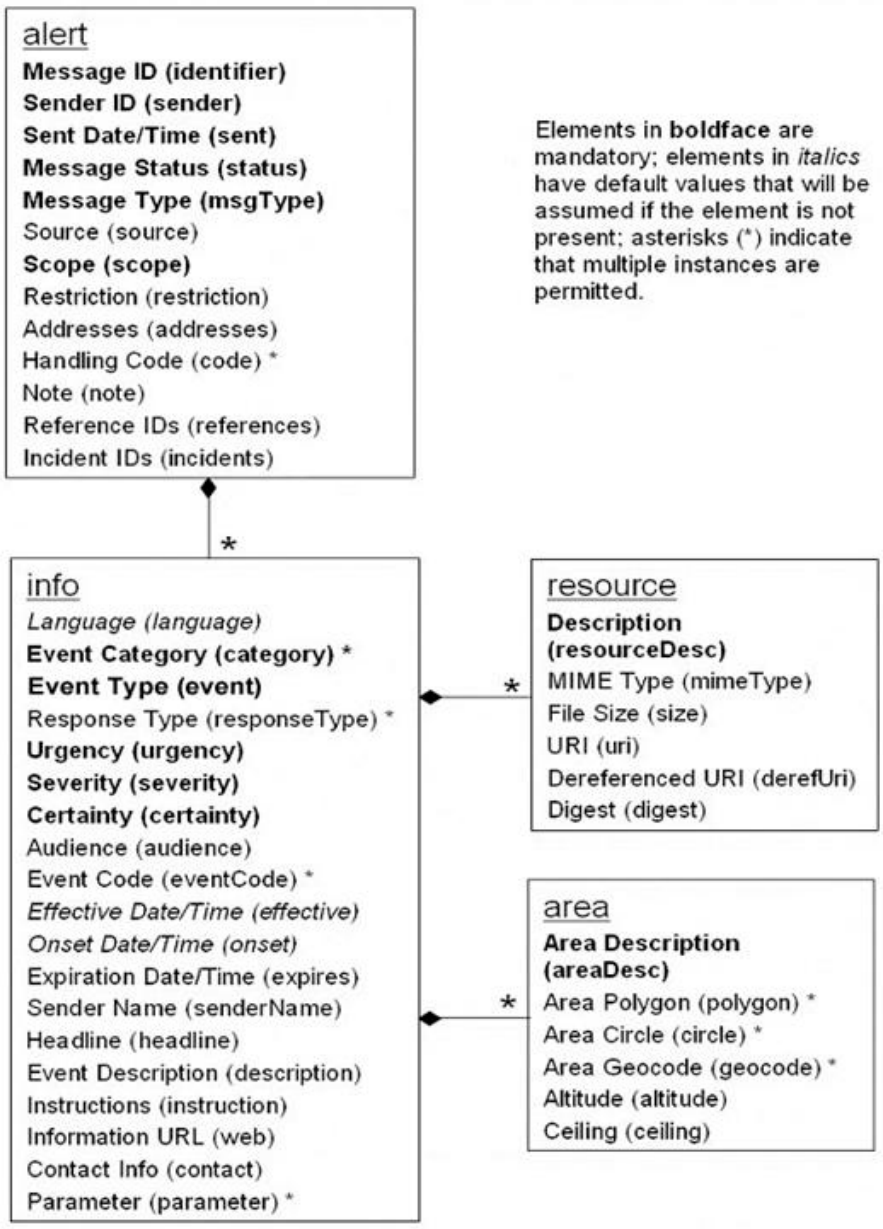

Figure 1 - CAP entity-relationship model[11]

[11] Full description of the attributes can be found at http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html.

5.1 <alert> - mandatory element

5.1.1 <identifier> – mandatory element

The <identifier> should always be laid out in the same way to create a unique code for each CAP message, which should also include the Alerting Authority Object Identifier (see Appendix B), date, time, and an extra unique component to differentiate two CAP messages from the same Authority issued at the same time.

For example, MetService also append event type (abbreviated) and area name (abbreviated):

<identifier>**2.49.0.0.554.0.tswarning.wl.20160821233954688.0**</identifier>

Table 4 - Explanation of MetService <identifier> element

Element	Description
2.49.0.0.554.0	Object Identifier (OID) of Alerting Authority (in this case, MetService); see Appendix B. (Note: this is not a valid OID string, but there is currently no simple method for referring to a valid OID string in CAP[12].)
tswarning	Abbreviated name for type of alert (in this case, thunderstorm warning).
wl	Abbreviation for which part of the country the alert applies to (in this case, Westland).
20160821233954688[13]	Date/time expressed as YYYYMMDDHHMMSSsss (in this case, 23:39:54 (and 688 milliseconds) UTC 21 August 2016).
0	Sequence number of alert issued in the millisecond specified above (in this case, numbered from 0).

If the agency uses any non-numeric, non-full stop (period) characters in addition to their official OID within the <identifier> element, then the OID cannot be prefixed with urn:oid. (The above example cannot use urn:oid for these reasons.)

For CAP originated in the New Zealand Red Cross web portal:

- the <identifier> element is always set to the New Zealand Red Cross Society Object Identifier only (i.e. it does not use the Alerting Authority's actual Object Identifier)
- the agency logged in to the web portal that has created the CAP message is instead uniquely identified by the <senderName> element, which is taken from the Alerting Authority's user account details.

[12] An Object Identifier (OID) on the internet is a registered type of URN (Uniform Resource Name). It should be so indicated by prefixing the OID with "urn:oid:". But there is no easy way of validly including *only* the OID as the <identifier> element of the CAP message because the content of this element for each CAP message must be unique.

[13] Note: do not parse the <identifier> string to extract time-values. The only valid time-values in the message are in the in <sent> and <effective> tags.

5.1.2 <sender> - mandatory element

An address that allows the recipient to seek further information. It is designed to allow people in the warning chain to get in touch with the sender.

The field can be seen publicly as it is a component of the CAP message. It is up to each Alerting Agency to decide whether this is populated with an email address, a phone number, a “Contact us” web page, etc. (*Note*: Any relevant website URL can be stored in the <web> sub-element of the <info> element; more usually, this is used as a link to the resource describing the event/actions.)

5.1.3 <sent> - mandatory element

The <sent> time is a date and time stamp in the format prescribed by the CAP DateTime data type. Alerting systems should present alert messages in the order of the <sent> time, *except* in the presence of an <effective> time.

5.1.4 <status> - mandatory element

The message status can be one of **Actual**, **Exercise**, **System**, **Test** or **Draft** - see the CAP standard for further details. Note Google require the use of ‘test’ for *all* test messages.

5.1.5 <msgType> - mandatory element

The message type can be one of **Alert**, **Update**, **Cancel**, **Ack** (acknowledge) or **Error** - see the CAP standard for further details.

5.1.6 <scope> - mandatory element, <restriction> conditional element and <addresses> - conditional element

The message scope can be one of **Public**, **Restricted** or **Private**. If **Restricted** use the <restriction> element to describe the rule for limiting distribution. If **Private** use <addresses> to limit distribution.

The <restriction> element allows an alert to indicate that it should only go to a sub-group of recipients. Without being hosted on a password-protected internet news feed, this is a request only and does not ensure restricted distribution. The OASIS standard states: “The text describing the rule for limiting distribution of the restricted alert message”. This functionality exists in CAP 1.2. If <restriction> is used, Alerting Authorities need to define, maintain and set up restriction lists as well as rules for their use.

5.2 <area> - mandatory element

The CAP <area> element is used for describing the threat (impact) area within which the message should be received, not the location of the subject event. The threat area and the event location can of course be very close spatially, but they may also be quite far apart. CAP does not currently have a data element specific to the subject event location. The optional <parameter> element allows for user-specified, system-specific elements.

The <area> element requires an area description at the very least. To describe an <area> precisely, use whichever of the <polygon>, <circle> and <geocode> elements are appropriate. Google state that they strongly prefer <circle> or <polygon> over <geocode>. Coordinate pairs

are decimal latitude and longitude values, e.g. -41, 175. A point can be described as a zero-radius <circle> element, or as a <geocode>.

If the area targeting of multiple <info> blocks in the same language overlaps, information in later blocks may expand but may not override the corresponding values in earlier ones. Each set of <info> blocks containing the same language identifier shall be treated as a separate sequence.

Further useful content can be found in Section 2.9 of CAP V1.2 Practices Guide Version 2.0[14].

5.2.1 <areaDesc> - mandatory element

The description of the effective area of the alert's impact must be given and be unambiguous. This is not a code but rather a short, plain-English statement to a public audience.

5.2.2 <polygon> - optional element

The paired values of points defining a polygon that delineates the affected area of the alert message:

1. The geographic polygon is represented by a whitespace-delimited list of coordinate pairs.
2. A minimum of four coordinate pairs *must* be present and the first and last pairs of coordinates *must* be the same.
3. Multiple instances *may* occur within an <area> block.
4. A counter-clockwise winding order is preferred.

Alerting Authorities should use the fewest number of polygons required to describe the area of the alert, and they must not overlap.

- Alerting Authorities should, if possible, use polygons which do not exceed 20 vertices per polygon.
- Any generalization of complex polygons should include all areas of the original polygon, and may therefore also include areas outside of it. However, overage should be kept to a minimum. *Alerting a slightly larger area is preferred to alerting an area less than that for which the alert has been issued.*
- Extremely complex but specific impact zones (e.g. a river floodplain) can be described by linking to or attaching a geographical format file in the <resource> element (not described here).

5.2.3 <circle> - optional element

The paired values of a point and radius delineating the affected area of the alert message:

1. The circular area is represented by a central point given as a coordinate pair followed by a space character and a radius value in kilometres.
2. Multiple instances may occur within an <area> block.

Circles are less desirable compared with polygons.

[14] https://www.oasis-open.org/committees/document.php?document_id=59021&wg_abbrev=emergency-cap

5.2.4 <geocode> - optional element

The geocode element allows for user-specified area descriptors to be shared between systems. This is primarily to support existing system interfaces. Ideally they would be accompanied by polygon or circle representations of the same area so as not to require specialist knowledge of the geocode scheme in use.

5.2.5 Standard area naming

The New Zealand Gazetteer of place names (http://www.linz.govt.nz/regulatory/place-names/find-place-name/new-zealand-gazetteer-place-names) is the authoritative list for places in New Zealand.

For regions, New Zealand has official regions that are defined under ISO-3166-2 (see https://en.wikipedia.org/wiki/ISO_3166-2:NZ). Other zonal boundaries are more appropriate for the event being reported. The ***CAP-NZ*** technical standard maintains Appendix I Region naming schemes used in New Zealand for all such area naming schemes and their scopes used by New Zealand Alerting Authorities.

5.2.6 WGS84 locations for New Zealand

Geographic locations in CAP are defined as latitude, longitude pairs using World Geodetic System 1984 abbreviated as **WGS84**. In New Zealand, any NZGD1949 and NZGD2000[15] latitude, longitude pairs should be transformed to WGS84 by the originator *before* insertion in a CAP message. Transformation and conversion must also be applied to projected coordinates such as New Zealand Map Grid (NZMG) and New Zealand Transverse Mercator (NZTM). The recommended transformations and conversions can be found at http://www.linz.govt.nz/data/geodetic-services/coordinate-conversion/online-conversions.

If the target area is not defined at an accuracy of less than one kilometre, then conversion to WGS84 is not considered necessary.

5.3 <info> - mandatory element

5.3.1 <category> - mandatory element

The <category> code(s) should be as correct as possible for any alerting systems that choose to use this element for processing and delivery of messages. Some events can have more than one category – for example, a landslide could be both Met (due to rainfall) and Geo (due to earthquake).

Table 5 - List of valid Category Codes

Category code	Description
Geo	Geophysical (including landslide)
Met	Meteorological (including flood)
Safety	General emergency and public safety
Security	Law enforcement, military, homeland and local/private security

[15] New Zealand Geodetic Datum 1949 and New Zealand Geodetic Datum 2000 respectively

Category code	Description
Rescue	Rescue and recovery
Fire	Fire suppression and rescue
Health	Medical and public health
Env	Pollution and other environmental hazards
Transport	Public and private transportation
Infra	Utility, telecommunication, other non-transport infrastructure
CBRNE	Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack
Other	Other events

5.3.2 <event> - mandatory element

This is the container for a descriptive term for the nature of the event, which in New Zealand should be chosen by matching it from the <eventCode> list (see Appendix C List of standard event codes for CAP-NZ).

5.3.3 <eventCode> - recommended element for New Zealand

Categories are too broad to be useful, so event codes are needed to provide additional specific detail.

The event description referred to by the <eventCode> should be the first word(s) in the <headline>, inserted in the <event> and also repeated in the <description>.

Any processing of the CAP message based on <eventCode> needs a single explicit code to look for. For example ‘flood’ is the standard code for all events that might colloquially be called ‘flood’, or ‘floods’, or ‘flooding’. Appendix C provides a lexicon for event codes in New Zealand.

They are best used by alerting dissemination platforms and end-points for:

- triggering appropriate instruction content (e.g. in an app; like the ‘what now’ content in the Red Cross Hazard app)
- making sure a configurable receiving system always propagates the correct types of alert. This would be impossible using the colloquial full message content.

5.3.4 <urgency>, <severity> and <certainty> - mandatory elements

These elements control whether an alert is less or more emphatic across a range of hazards. Detail about these elements can be found in Section 4.

5.3.5 <effective> - recommended element for New Zealand

The <effective> time, a CAP DateTime data type, is when the information of the alert message becomes effective. Note that the <effective> time takes precedence over the <sent> time.

5.3.6 <expires> - recommended element for New Zealand and <responseType> - recommended element for New Zealand

<expires> is the expiry date and time of the information in the alert message. It is *not* the expected end time of the event, *nor* is it the time when an update message can be expected to supersede this message.

Section 3.5 of the CAP V1.2 Practices Guide Version 2.0[16] contains further information about the use of an event expiration parameter. The following useful points are given here:

- Alerting Authorities are responsible for ensuring their alert messages are expired or cancelled
- the effective time of an alert message may be ended by issuing an alert <msgType> value **Update** with an <expires> value set to the current or near current time, and the appropriate reference to the alert the cancel or update refers to
- the inclusion of an **AllClear** <responseType> is highly encouraged.

A hazard passing through multiple areas of differing impact can be represented by multiple <info> blocks. As the hazard passes, these <info> blocks can be progressively expired or given the “all clear”.

5.3.7 <senderName> - recommended element for New Zealand

This should be the Alerting Authority’s proper name. (Note the OID goes in <identifier>, not here.)

5.3.8 <headline> – recommended element for New Zealand

At a minimum, the <headline> element should contain all key messages for those display or broadcast systems that do not carry more than 140 characters; this is consistent also with Google Public Alerts guidance. *This especially applies to Twitter and SMS, but is also important for mobile apps* because the critical initial smartphone locked screen version of an app push notification is of a short character length.

The sequence and content should include (as applicable to the event) all of:

- **alerting agency**
- **hazard (<event code>)**
- **time**
- **location**
- **urgency statement**
- **action**

Useful information about constructing short messages can be found at https://www.internetalerts.org/fia_documents/warning-design-guidelines_012015.pdf.

5.3.9 <description> - recommended element for New Zealand and <instruction> - recommended element for New Zealand

Every CAP alert should include content in a ‘what happened’ / ‘is expected to happen’ <description> element and a ‘call to action’ <instruction> element. Google Public Alerts states that

[16] https://www.oasis-open.org/committees/document.php?document_id=59021&wg_abbrev=emergency-cap

the <instruction> and <description> text must not be the same. When originating CAP messages Alerting Authorities should have templates for the content of the <description> and <instruction> elements. For natural hazard or pandemic warnings, these should be consistent with MCDEM's *Consistent messages for CDEM*, available at www.civildefence.govt.nz on the Publications page. All public messages including warnings should be written in plain English, that all members of the public can easily understand.

Care should be taken to discuss, agree and attribute the correct portion of the CAP message with the agency responsible for the origination of that part of the messaging (especially *description-incident* vs *instruction-life safety components*). For example, for earthquakes from GNS Science's CAP feed (see Appendix F), Google Public Alerts credits GNS Science with the <description> and MCDEM with the <instruction>.

5.3.10 <language> element – optional element

Support for Maori language (specifically macronised vowels – e.g. 'Māori') is mandatory in any CAP system. This is best achieved by systems having full UTF-8 support, not just plain ASCII, ensuring any alerting system instigated in New Zealand is Māori language-capable.

Multiple <info> blocks are permitted within a single <alert>. This is especially useful in New Zealand for provision of separate Māori and English versions of the alert info block.

Section 6 Delivering CAP to display or broadcast systems

6.1 Accommodating a range of alerting end points

In New Zealand CAP messages need to be usable across a range of alerting display or broadcast technologies. This includes text displayed on systems such as digital road signs, text messages, cell broadcast messages (Emergency Mobile Alerts), app screens, as well as the ability to utilise maps and URLs referred from within single or multiple CAP messages. These vary in terms of message length display and whether they can accommodate rich content such as images, audio and video. See Appendix D Display and broadcast constraints for currently identified constraints.

For example, SMS text messages, Twitter and first generation cell broadcast messages have a limit of about 140 characters, whereas mobile apps can carry thousands of characters and rich content (although the push notification to a smartphone is often only initially visible with a restricted number of characters).

In order to accommodate all known and emerging technologies in an ideal way the CAP <headline> must include a sufficient summary of the <instruction> and <description> elements necessary to trigger effective warning response in the public.

The <description> and <instruction> elements themselves should contain more detail, to be available for any systems that can accommodate this.

It is understood that length and or duration of message may be truncated by alerting systems due to their technical constraints. Alerting Authorities are therefore encouraged to place the most important information at the beginning of the message to ensure that the most critical information is presented should their text, audio or video exceed the presentation constraints of an alerting system.

It is understood that some alerting endpoint applications may be programmed to interpret space, carriage return, new line, etc. in the CAP free form text elements as a single space. Recognizing the number of media that a single audience alert message may be distributed through, all alert originating parties, including re-originators, should be aware that conventions that work on one type of display media may have unexpected results on others. *Hence special interpretations of characters within a standard message is not recommended.*

6.2 High-priority alerts

These are intrusive alerts that must go to all alerting end points without the option of opting out, with a different heads-up where possible (e.g. siren sound on the Red Cross app, unique sound and length for Emergency Mobile Alerts).

6.3 Message updates

When an alerting system receives an update alert message for an alert message that they intend to present and have not yet presented, the end point should present the updated alert message only.

6.4 Speed of delivery

Once an alert message has been published, every party involved in the distribution of that alert should work towards advancing and presenting the audience alert message to the public with as little delay as possible.

6.5 Alerting attention signal

Consider using a tone that attracts attention. For example, a Civil Defence alert tone[17] is played on radio stations introducing civil defence emergency messages, and Emergency Mobile Alerts have a standard sound on all handsets. High-priority alerts may be associated with these deliberately-intrusive tones.

6.6 Audio content considerations

- Alerting Authorities should aim to deliver the content of their audio message in less than 60 seconds per language.
- Audio content should be made available to end points as a monophonic MP3 file, using a coding rate of at least 64 kbit/s data.
- Other audio formats may also be supported, depending on the broadcast system.
- Be sure that audio files' size do not exceed the broadcast system constraints.
- Alerting Authorities should not include an alerting attention signal in the audio file associated with an audience alert message; this should be provided separately.
- In the absence of a suitable audio file, systems with audio capabilities are encouraged to read the text found in the CAP <description> element or use text-to-speech functionality. A standard message is a least preferred option, although it is recognized to be better than no audible message.

6.7 Other system specific considerations

These will be considered in later versions of the ***CAP-NZ*** technical standard as Alerting Authorities acquire more experience with implementing CAP – please refer to Appendix E CAP-NZ alerting trigger levels.

[17] http://getthru.govt.nz/themes/getthru/templates/vwluResources/Siren/$file/Siren.wav

Section 7 Appendices

Appendix A About the CAP-NZ Working Group

In recognition of the importance of interoperable emergency communications to the safety and security of New Zealanders, a New Zealand Common Alerting Protocol Working Group was assembled in December 2015. It was jointly led by MetService and GNS Science until December 2016, thereafter chaired by the Ministry of Civil Defence & Emergency Management.

It is made up of New Zealand agencies, groups, individuals and companies responsible for the creation and/or dissemination of alerting messages. Its purpose is to use CAP as the standard for effective message interchange.

The Working Group develops, agrees and maintains the ***CAP-NZ*** technical standard, education, uptake and consistency of CAP across alerting agencies, software developers and hardware manufacturers.

It submits New Zealand's recommendations for improvement of the CAP standard to OASIS (Organization for the Advancement of Structured Information Standards) through its national representative.

All data, tools and documentation are free and open for the benefit of all New Zealanders.

To join the Working Group, receive minutes of its proceedings, provide feedback or for any further details, please contact:

National Operations
Ministry of Civil Defence & Emergency Management
PO Box 5010, Wellington 6145
New Zealand

Phone +64 4 817 8555

Email emergency.management@dpmc.govt.nz

Appendix B Registration as an Alerting Authority

The World Meteorological Organization (WMO) and the International Telecommunications Union (ITU) maintain an international Register of officially recognised Alerting Authorities[18].

The Register exists because there is a need for aggregators and other intermediaries to identify authoritative sources of alert messages. Each Register entry asserts that a particular source of alert messages is regarded by a WMO Member State as authoritative. New Zealand is a WMO Member State.

Entries in the Register can only be added or changed by an editor officially designated by the Permanent Representative of New Zealand with WMO. The position of Permanent Representative is held by the Chief Executive of MetService and the Registry editor is a staff member of MetService.

Official New Zealand Alerting Authorities should uniquely identify themselves via their assigned Object Identifier (OID) in the <identifier> element – see 5.1.1. The OID will be of the form 2.49.0.0.554.{x.y(.z)}.

B.1 Obtaining an Object Identifier

1. The organisation seeking an Object Identifier (OID) must make a formal application in writing to the Permanent Representative of New Zealand with World Meteorological Organization (WMO) for addition to the New Zealand section of the Register of Alerting Authorities. This formal application must include:
    (a) The full name of the organisation seeking addition and the person making the application
    (b) References to the relevant New Zealand law(s) or regulation(s) establishing the organisation seeking addition as an Alerting Authority. Typically, this will include appropriate text from clause 120 and/or clause 124 of the National Civil Defence Emergency Management Plan[19]
    (c) Description of the nature of the alerting messages the organisation seeks official designation for (e.g., "Earthquake - lead agency").
2. MetService will forward applications for addition to the New Zealand section of the Register of Alerting Authorities to MCDEM. MCDEM will decide whether or not it is appropriate for the organisation seeking addition to the Register to be assigned an identifying OID of the form 2.49.0.0.554.{x.y(.z)} and advise MetService accordingly.
3. If it is appropriate for the organisation to be added to the Register, MetService will formally and in writing advise the organisation (with a copy to MCDEM), via the Permanent Representative of New Zealand with WMO, of New Zealand's agreement to:
    (a) Assign an identifying OID of the form 2.49.0.0.554.{x.y(.z)} to the organisation, and
    (b) Add the organisation to the Register of Alerting Authorities.

    Subsequently, MetService will:
    (c) Assign an identifying OID of the form 2.49.0.0.554.{x.y(.z)} to the organisation

[18] http://alerting.worldweather.org/

[19] https://www.civildefence.govt.nz/cdem-sector/cdem-framework/national-civil-defence-emergency-management-plan/

(d) Advise WMO, via the Permanent Representative of New Zealand, of New Zealand's intention to add the organisation to the Register of Alerting Authorities with the assigned OID

(e) Add the organisation to the Register of Alerting Authorities

(f) Submit a validation request to the OID Repository for the organisation's identifying OID number

(g) Advise MCDEM who will update Table 6 in this document.

4. If MCDEM decides it is not appropriate for the organisation to be added to the Register, MetService will formally and in writing advise the organisation (with a copy to MCDEM), via the Permanent Representative of New Zealand with WMO, that the request for an identifying OID will not be granted, with MCDEM's supporting reasons.

Table 6 - New Zealand Registered Alerting Authorities

OID Number	Alerting Authority	Hazard Categories
2.49.0.0.554.0	MetService	Met
2.49.0.0.554.1	GNS Science	Geo
2.49.0.0.554.2 2.49.0.0.554.2.1 2.49.0.0.554.2.2 2.49.0.0.554.2.3 2.49.0.0.554.2.4 2.49.0.0.554.2.5 2.49.0.0.554.2.6 2.49.0.0.554.2.7 2.49.0.0.554.2.8 2.49.0.0.554.2.9 2.49.0.0.554.2.10 2.49.0.0.554.2.11 2.49.0.0.554.2.12 2.49.0.0.554.2.13 2.49.0.0.554.2.14 2.49.0.0.554.2.15 2.49.0.0.554.2.16 2.49.0.0.554.2.17	MCDEM Northland CDEM Group Auckland CDEM Group Waikato CDEM Group Bay of Plenty CDEM Group Gisborne CDEM Group Hawkes Bay CDEM Group Manawatu-Whanganui CDEM Group Taranaki CDEM Group Wellington CDEM Group Nelson-Tasman CDEM Group Marlborough CDEM Group Canterbury CDEM Group West Coast CDEM Group Otago CDEM Group Southland CDEM Group Chatham Islands CDEM Group Other	Geo, Met, Safety, Infra
2.49.0.0.554.3	Ministry of Health	Health, Env, CBRNE
2.49.0.0.554.4	Fire and Emergency New Zealand	Fire
2.49.0.0.554.5	New Zealand Police	Env, CBRNE, Infra, Rescue, Security
2.49.0.0.554.6	New Zealand Transport Agency	Transport
2.49.0.0.554.7	Ministry for Primary Industries	Health, Env
2.49.1.127	New Zealand Red Cross	

B.2 Object Identifiers for Lifelines Utilities

There are a multiplicity of organisations, both public and private, supporting lifelines in New Zealand. This precludes pre-registration of all of them. Instead, MCDEM will consider Object Identifiers for any lifeline organisation that meets condition 1 (b) above, as their need arises.

Appendix C List of standard event codes for CAP-NZ

This is a controlled list of values of <eventCode> for New Zealand CAP. *It is incomplete, and is developed as Alerting Authorities move to CAP authoring.*

The <eventCode> element consists of a <valueName> and <value> pair. The <valueName> is set to **eventCode** and the <value> selected from the following list. An example for *Storm Surge* is shown below.

```
<eventCode>
   <valueName>eventCode</valueName>
   <value>stormSurge</value>
</eventCode>
```

Table 7 - New Zealand's event codes

Tier I Events (includes associated Tier II events)	Tier II Events (included in Tier I event associated with it)	Event Code	Hazard Category
Aviation	Airport Lightning Threat	avLightning	Met
Aviation	Airport Thunder Threat	avThunder	Met
Fire	Fire Weather	fireWeather	Met
Flood	-	flood	Met
Flood	Flash Flood	flashFlood	Met
Flood	High Water Level	highWater	Met
Flood	Storm Surge	stormSurge	Met
Flood	River Flood	riverFlood	Met
Geophysical	Earthquake	earthquake	Geo
Geophysical	Tsunami	Tsunami	Geo
Geophysical	Land Threat Tsunami	landTsunami	Geo
Geophysical	Beach Threat Tsunami	beachTsunami	Geo
Marine	-	marine	Met
Marine	Gale Wind	galeWind	Met
Marine	Hurricane Force Wind	hurricFrcWnd	Met
Marine	Iceberg	iceberg	Met
Marine	Large Coastal Surf	largeSurf	Met
Marine	Large Swell Waves	largeSwell	Met
Marine	Squall	squall	Met
Marine	Storm Force Wind	stormFrcWind	Met
Marine	Strong Wind	strongWind	Met
Marine	Waterspout	waterspout	Met

Tier I Events (includes associated Tier II events)	Tier II Events (included in Tier I event associated with it)	Event Code	Hazard Category
Storm	-	storm	Met
Storm	Hail	hail	Met
Storm	Rainfall	rainfall	Met
Storm	Snowfall	snowfall	Met
Storm	Thunderstorm	thunderstorm	Met
Storm	Tornado	tornado	Met
Storm	Tropical Cyclone	tropCyclone	Met
Storm	Tropical Storm	tropStorm	Met
Storm	Winter Storm	winterStorm	Met
Storm	Weather	weather	Met
Temperature	-	temperature	Met
Temperature	Cold Outbreak	coldOutbreak	Met
Temperature	Heat Wave	heatWave	Met
Temperature	Frost	frost	Met
Temperature	Wind Chill	windChill	Met
Wind	-	wind	Met

Appendix D Display and broadcast constraints

The most common constraints on message display and broadcast are listed below:

D.1 Display device

Short Message Service (SMS)

- 160 characters in one message
- Maximum is 918 characters sent as six chunks of 153 characters.

Twitter

- 140 characters limit
- Consider room for hashtags of the re-tweeter
- Use of URL shortening services can significantly reduce characters required for long web links.

Cell Broadcast (known as Emergency Mobile Alert)

- Standard limit of 1,395 characters; in New Zealand, this limit is 930 characters due to technology constraints
- Proposal[20] in the United States to advance functionality to include small images (e.g. for missing person alerts) and clickable URLs.

D.2 Broadcast device

These are constraints used in the United States[21], which are a sensible place to start. It includes suggestions as to how to construct the full message from various CAP elements:

- Maximum 1,800 characters *total* message length
- Maximum 120 seconds audio.

Digital Road Sign

These are set up manually, so any message would be tailored to suit the available display space.

Television and Radio

Audio content that is to be distributed over TV and radio must not exceed 120 seconds in length.

[20] https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-127A1.pdf

[21] ECIG Recommendations for a CAP EAS Implementation Guide, Version 1.0 17 May 2010

Appendix E CAP-NZ alerting trigger levels

In order to help define consistent use of the three core elements *urgency*, *severity* and *certainty*, some consideration of alerting systems and their behaviour is useful.

The *CAP Trigger Levels Matrix task group* is developing a matrix that compares different intensities for a variety of hazards, against the desired behaviour of alerting systems, aiming for a consistent application of these core levels across the hazards.

For each agency, it considers the event that is being alerted, the level of the alert in their local terminology (referred to as the *package name*: report, advisory, watch, warning, bulletin, etc.), the local metrics used, the time within which the alert level can be expected to be reached, its certainty, and the scale of area typically affected.

Agencies map their package names and metrics to the CAP elements of urgency, severity and certainty, and consider the triggers that cause these alerts to be issued.

Display and broadcast options are also considered, and agencies choose which alerts would go to each of these systems. For example, if an alert is going to be displayed within an app, it can feature a number of CAP elements. If it is going to a roadside sign, it may only show part of the headline element. A tone siren will display nothing at all.

The task group will create a decision matrix to summarise this research.

Appendix F Example of a CAP template – NZ message

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>2.49.0.0.554.0.severeweather.nz.20180118201933455.4</identifier>
  <sender>http://www.metservice.com</sender>
  <sent>2018-01-19T09:19:33+13:00</sent>
  <status>Actual</status>
  <msgType>Update</msgType>
  <scope>Public</scope>
  <references>
http://www.metservice.com,2.49.0.0.554.0.severeweather.nz.20180118073504396.5,2018-01-
18T20:35:04+13:00
  </references>
  <info>
    <category>Met</category>
    <event>rain</event>
    <responseType>Monitor</responseType>
    <urgency>Immediate</urgency>
    <severity>Moderate</severity>
    <certainty>Likely</certainty>
    <onset>2018-01-19T09:00:00+13:00</onset>
    <expires>2018-01-19T14:00:00+13:00</expires>
    <senderName>Meteorological Service of New Zealand Limited</senderName>
    <headline>Heavy Rain Warning</headline>
    <description>
Periods of northerly rain expected to ease early this afternoon. During this period a
further 20 to 30 mm is expected to accumulate about the eastern areas and lesser amoun
ts elsewhere. Peak intensities of 10 to 20mm/hr in isolated heavy falls.
    </description>
    <instruction>
Note: A Severe Weather Warning or Watch means conditions are favourable for severe wea
ther in and close to the indicated area. People in these areas should be on the lookou
t for threatening weather conditions and monitor for further updates from MetService.


For information on preparing for and keeping safe during a       storm, see the Civil
Defence Get Ready Get Thru website.
    </instruction>
```

```
    <web>http://metservice.com/warnings/severe-weather-warnings</web>
    <parameter>
      <valueName>NextUpdate</valueName>
      <value>2018-01-19T21:00:00+13:00</value>
    </parameter>
    <area>
      <areaDesc>Northland, mainly about eastern areas.</areaDesc>
      <polygon>
-36.345,173.996 -36.263,173.969 -36.012,173.771 -35.650,173.427 -35.532,173.335 -35.39
0,173.206 -35.298,173.137 -35.206,173.048 -35.171,173.038 -35.144,173.064
-35.155,173.114 -35.147,173.137 -35.082,173.153 -35.033,173.147 -34.911,173.067 -34.64
8,172.843 -34.480,172.625 -34.466,172.621 -34.447,172.654 -34.403,172.671
-34.433,172.800 -34.401,172.853 -34.406,172.955 -34.376,173.018 -34.392,173.051 -34.41
7,173.067 -34.425,173.064 -34.436,173.028 -34.550,173.015 -34.591,173.018
-34.700,173.087 -34.757,173.170 -34.798,173.190 -34.830,173.186 -34.863,173.239 -34.87
1,173.272 -34.857,173.269 -34.849,173.275 -34.825,173.365 -34.792,173.365
-34.765,173.404 -34.833,173.484 -34.868,173.484 -34.901,173.401 -34.930,173.401 -34.96
3,173.431 -34.968,173.503 -34.939,173.510 -34.898,173.560 -34.939,173.708
-34.976,173.731 -34.993,173.768 -34.979,173.804 -34.979,173.834 -34.960,173.867 -34.97
4,173.880 -34.998,173.873 -35.001,173.880 -34.993,173.893 -34.998,173.903
-34.955,173.930 -34.968,173.986 -35.039,173.986 -35.058,173.953 -35.071,173.953 -35.09
3,173.969 -35.101,173.999 -35.101,174.082 -35.114,174.101 -35.133,174.115
-35.144,174.148 -35.168,174.154 -35.190,174.121 -35.214,174.125 -35.233,174.088 -35.23
1,174.138 -35.179,174.204 -35.195,174.260 -35.166,174.280 -35.150,174.352
-35.212,174.352 -35.276,174.339 -35.328,174.409 -35.400,174.399 -35.433,174.455 -35.51
6,174.498 -35.532,174.485 -35.543,174.491 -35.538,174.511 -35.583,174.564
-35.650,174.554 -35.667,174.537 -35.693,174.544 -35.707,174.587 -35.795,174.580 -35.83
5,174.607 -35.865,174.607 -35.878,174.541 -35.868,174.504 -35.929,174.491
-36.007,174.524 -36.031,174.604 -36.071,174.630 -36.167,174.485 -36.268,174.323 -36.34
0,174.065 -36.345,173.996
      </polygon>
    </area>
  </info>
</alert>
```

Appendix G Acronyms and definitions

Agency - any formal group, company involved in the dissemination of public alerts; government or otherwise. Here it is a synonym of *Organisation*.

Alert – a notification that is also an alarm.

Alerting Authority – an organisation with official authority to originate public alerts, registered on the World Meteorological Organization Register of Alerting Authorities[22].

Atom – the Atom Syndication Format is an XML language used for web feeds.

CAP – Common Alerting Protocol. An open XML standard for alert messages[23].

CAP Hubs - CAP Hubs are software running on internet-connected servers that scrape individual internet news feeds and aggregate them to a single Hub internet news feed. Alerting end-points monitor the hubs for alerts that apply to their search parameters, and send the alerts to the public. Scrape means to continuously monitor the feed and take up new content when it is published.

CAP-NZ Working Group – The New Zealand CAP Working Group, an open group of private and government organisations in New Zealand that maintains this technical standard. The Business Owner for the Working Group is MCDEM.

CAP validation – Validation of a CAP message ensures that it is correctly formatted. It can be done at: https://cap-validator.appspot.com/.

Digital signature - A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

Element – A part of a CAP message with the element name written between two triangular parentheses < >. The CAP standard prescribes the name, content description and whether the element is optional or required.

Emergency – An emergency means a situation that:

(a) is the result of any happening, whether natural or otherwise, including, without limitation, any explosion, earthquake, eruption, tsunami, land movement, flood, storm, tornado, cyclone, serious fire, leakage or spillage of any dangerous gas or substance, technological failure, infestation, plague, epidemic, failure of or disruption to an emergency service or a lifeline utility, or actual or imminent attack or warlike act, and

(b) causes or may cause loss of life or injury or illness or distress or in any way endangers the safety of the public or property in New Zealand or any part of New Zealand, and

(c) cannot be dealt with by emergency services, or otherwise requires a significant and coordinated response under the New Zealand CDEM Act 2002.

Emergency Mobile Alert – New Zealand's name for a short alert message issued using cell broadcast technology.

Event - An event is any situation that a CAP message may need to be generated for. Most events that require CAP messages in New Zealand are expected to be emergencies.

FIA – Federation of Internet Alerts (https://www.internetalerts.org/).

[22] http://alerting.worldweather.org/

[23] http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

GCDO – Government Chief Digital Officer (and team) in New Zealand (https://www.ict.govt.nz/governance-and-leadership/the-gcio-team/).

Google CAP definition – a definition statement from Google Public Alerts (https://developers.google.com/public-alerts/?visit_id=0-636515753538364140-3453619722&rd=1).

HTML - Hyper Text Markup Language, the standard markup language for creating web pages. The structure of a web page is made up of HTML elements.

MCDEM – The Ministry of Civil Defence & Emergency Management in New Zealand.

Monitoring Agency – An official monitoring agency defined in the National CDEM Plan.

Notification – a specific piece of information that serves to notify.

OASIS - Organisation for the Advancement of Structured Information Standards.

OID - In computing, an object identifier or OID is a standard identifier used to name an object (http://www.oid-info.com/standards.htm).

Organisation – Any formal group, company involved in the dissemination of public alerts; government or otherwise. Here it is a synonym of Agency.

Originate – To generate a validated CAP message. This is usually done either automatically by software or manually by a person using a form on a computer.

Origination platform – automatic code, or an HTML form, that generates validated CAP.

Public alert – Any alert intended for the public. These should be transmitted to alerting systems or hardware in CAP format, but should reach the public as clear human-sensed messages.

Public alert redistributor – Any vendor that ingests CAP messages and passes them on to other redistributors or to alerting end points.

Public alerting end point – Any piece of technology that ingests CAP messages and delivers them to the public as clear human-readable messages.

Register of Alerting Authorities –The World Meteorological Organization-maintained register, administered by MetService in coordination with MCDEM in New Zealand.

RSS – Rich Site Summary – uses a standard web feed format, usually XML, to publish frequently updated information. It is usually accessed via a standard website URL. CAP alerts are usually supplied originally as RSS feeds.

URL - A Uniform Resource Locator (URL), commonly informally termed a web address, is a reference to a web resource that specifies its location on a computer.

Warning – A general term that refers to any or all elements (depending on who is using the term) in the chain from detection through to public alerting of (and response to) an event.

WMO – World Meteorological Organization.

XML - XML stands for eXtensible Markup Language. XML was designed to store and transport data. XML was designed to be both human- and machine-readable.

Appendix H List of current Alerting Authorities and systems using CAP

Table 8 - New Zealand's currently live CAP feeds

Alerting Authority	CAP feed	Hazard	Known current uses
GNS Science	http://api.geonet.org.nz/cap/1.2/GPA1.0/feed/atom1.0/quake	Earthquake	Red Cross app Google Public Alerts Federation for Internet Alerts
MetService	http://alerts.metservice.com/cap/rss	Severe weather	Red Cross app
CDEM Groups (via the New Zealand Red Cross web portal)	https://api.preparecenter.org/v1/org/nzl/alerts/rss	Multiple hazards	Red Cross app

Appendix I Region naming schemes used in New Zealand

I.1 Regional councils, unitary authorities, and special island authority

New Zealand has official regions that are defined under ISO-3166-2 (see https://en.wikipedia.org/wiki/ISO_3166-2:NZ).

Table 9 - New Zealand's official regional names

Code	Subdivision name	Subdivision name	Subdivision category
NZ-AUK	Auckland	Tāmaki-makau-rau	region
NZ-BOP	Bay of Plenty	Te Moana a Toi Te Huatahi	region
NZ-CAN	Canterbury	Waitaha	region
NZ-GIS	Gisborne	Tūranga nui a Kiwa	region
NZ-HKB	Hawke's Bay	Te Matau a Māui	region
NZ-MBH	Marlborough		region
NZ-MWT	Manawatu-Wanganui	Manawatu Whanganui	region
NZ-NSN	Nelson	Whakatū	region
NZ-NTL	Northland	Te Tai Tokerau	region
NZ-OTA	Otago	Ō Tākou	region
NZ-STL	Southland	Murihiku	region
NZ-TAS	Tasman		region
NZ-TKI	Taranaki	Taranaki	region
NZ-WKO	Waikato	Waikato	region
NZ-WGN	Wellington	Te Whanga-nui-a-Tara	region
NZ-WTC	West Coast	Te Taihau ā Uru	region
NZ-CIT	Chatham Islands Territory	Wharekauri	special island authority

Appendix J Recommended documents

J.1 Fundamental definition

The OASIS standard definition of CAP can be found at http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html

J.2 Best practice

The following documents provide some additional guidance on good practice when implementing the OASIS standard:

- *Common Alerting Protocol V1.2 Practices Guide Version 2.0* https://www.oasis-open.org/committees/document.php?document_id=59021&wg_abbrev=emergency-cap
- Federation of Internet Alerts (FIA) guidance https://www.internetalerts.org/fia_documents/warning-design-guidelines_012015.pdf
- Google CAP guidance https://developers.google.com/public-alerts/guides/introduction
- *Google Public Alerts Technical Guide* https://docs.google.com/document/pub?id=1J7bz05S6C1c5WvCd4m6f9asGoKqUpa2OUsaqx4SPKzM

J.3 Overseas implementations

- *United States* https://www.fema.gov/common-alerting-protocol
- *Canada* https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/capcp/index-en.aspx and https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ntnl-pblc-lrtng-sstm-eng.aspx
- *Australia* http://docs.oasis-open.org/emergency/edxl-cap1.2-au/v1.0/cs01/edxl-cap1.2-au-v1.0-cs01.html

J.4 Message contents

Consistent messages for Civil Defence Emergency Management http://www.civildefence.govt.nz/cdem-sector/consistent-messages-for-cdem/.

Design of messages https://www.internetalerts.org/fia_documents/warning-design-guidelines_012015.pdf.

J.5 Public alerting options in New Zealand

Wright, K.C.; Leonard, G.S.; Beatson, A.; O'Sullivan, R.; Coomer, M.A.; Morris, B.; Freire, D. 2014 Public alerting options assessment : 2014 update. GNS Science report 2014/66: http://shop.gns.cri.nz/sr_2014-066-pdf/

J.6 Display and broadcast equipment constraints

- *United States* Emergency Alert System/CAP Industry Group (ECIG): ECIG Recommendations for a CAP EAS Implementation Guide, Version 1.0: https://www.fema.gov/pdf/emergency/ipaws/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf
- *Canada* Common Look and Feel Guidance Version 1.2: https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/npas/clf-lng-12-en.aspx