

Scope of Services, Expected Outputs and Target Completion

SYSTEM DEFINITION

The CAP Server system hereby to referred as “CAP Server” in this document is a combination of two (2) CAP Server devices. The Primary CAP Server is the Server installed physically in country and the Secondary or Backup CAP Server is a server meeting the exact operational specifications as the Primary CAP Server in a geographically separate location. The Secondary server is to be implemented as a virtual server on a physical device. This physical device will host multiple virtual servers i.e. the secondary servers for each country. This configuration would allow the required level of redundancy for each country while reducing hardware and software costs as much as possible. With this mechanism the warning system can continue to function in the face of a temporary outage of either CAP server.

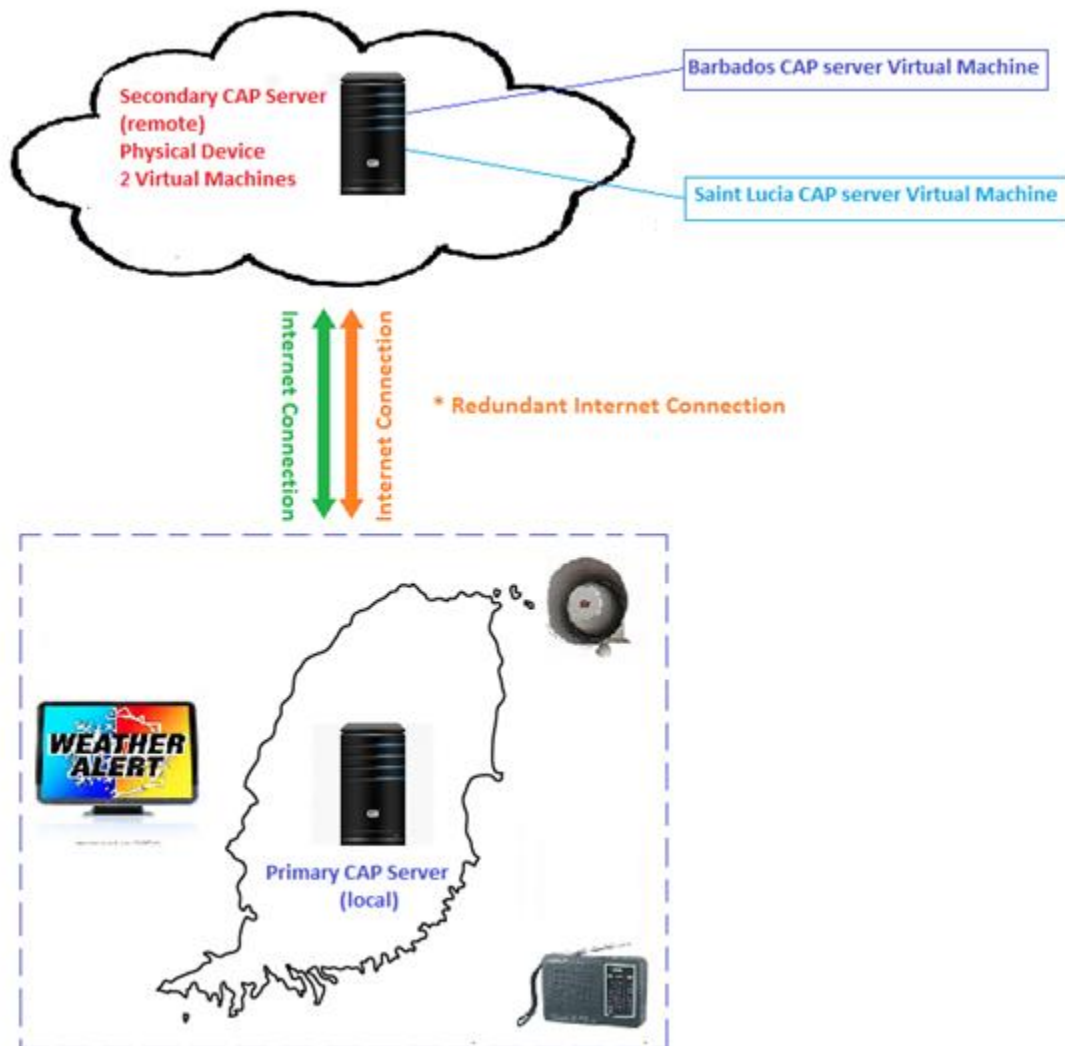


Figure showing System Configuration

1. CAP SERVER SYSTEM FUNCTIONALITY

- (a) Both servers are online, fully functional and can be utilised independently at any point to perform any task as outlined in the specifications.
- (b) The servers will sync databases for emails, alerts, system configuration and messages templates according to the following schedule :
 - (i) Immediately when any configuration change is made to either server.
 - (ii) Immediately when any alert is sent from either server.
 - (iii) Every 60 minutes to ensure database consistency
 - (iv) In the event of any sync failure sync will be reattempted every 60 seconds until the sync is complete.
- (c) All sync events and failures will be logged and a notification email sent to Administrators notifying of sync failures.
- (d) The CAP server will employ a “watchdog” function which continually monitors the health of both servers and their availability. The watchdog will immediately notify the Administrators of the system of any failure or unexpected condition via email.
- (e) All alerts processed by the CAP Server are formatted according to OASIS Common Alerting Protocol (CAP) version 1.2 specifications; except that new alerts submitted using a web form are accepted in HTML multipart form format and are converted immediately into CAP 1.2 format prior to further processing.
- (f) The CAP Server provides network interfaces for:
 - (i) Alert submission (for original and forwarded alerts). (please refer to web alert origination subsystem and Application Programming Interface below)
 - (ii) Public alert publication to the general Internet; and,
 - (iii) Directed alert forwarding to specified devices including in-Country specific dissemination systems and other networked CAP Servers.
- (g) The CAP Server detects duplicate CAP alerts by comparing the combination of the message’s CAP **sender**, **identifier** and **sent** values on each alert received with a record of previously received messages, and discard any duplicate messages without further processing.
- (h) The CAP Server shall maintain a completely auditable record of all alerts received, published and routed, and of all system errors including authentication failures. Such records are maintained within the CAP Server for a minimum of twelve (12) months, and a method is provided for transferring older records to external archival storage prior to their deletion. Records will not be automatically deleted by the system unless their storage can adversely affect the performance of the machine. In this case messages will be deleted on a least recently created basis.

- (i) The CAP Server shall provide web-based mechanisms by which only authenticated administrators can:
 - (i) Add, edit and delete authorizations for users and devices, including other CAP Servers to submit alerts to the Server.
 - (ii) Specify whether alerts received from each authorized device via the API can be automatically dispatched on receipt or be delivered to an “inbox” where they can be manually dispatched or discarded as required.
 - (iii) Manage X.509 certificate generation, archiving and certificate revocation for that system.
 - (iv) Add, edit and delete policies to be applied by the CAP server in the forwarding of alerts to dissemination systems or other servers, including thresholds, geocodes and other filtering criteria and any necessary routing and authentication information.
 - (v) Add, edit and delete alerting zone definitions which shall include CAP areaDesc, geocode and geometry (polygon and/or circle values)
 - (vi) Add, edit and delete pre-written, alert templates including selection of alert dissemination methods, attachment of MultiMedia as described in the section MultiMedia Formats and the selection of values for other custom parameters as defined in these specifications. Each alert template on the system shall have a unique name.
 - (vii) Add, edit and delete alert dissemination methods available for use on the system i.e. AlertMechanismName and FriendlyNames in accordance with the section “Custom Parameters”
 - (viii) Disable built-in alerting mechanisms i.e. email and smartphone applications
 - (ix) View and export to archival storage the log of all system activities and errors; and
 - (x) Conduct any other system configuration or administration functions.
- (j) The CAP Server shall provide a web based mechanism by which only authorized originators may create, review and release new alerts as described in the section **“Web Alert Origination Subsystem”** below.
- (k) The CAP Server shall automatically logout out users from interfaces after fifteen (15) minutes of inactivity.

2. TELECOMMUNICATION AND DATA TRANSFER PROTOCOLS

- (a) All interfaces to the CAP Server shall be implemented using Internet-compatible TCP/IP communications over Ethernet adapters. Both IP versions 4 and 6 are to be supported.
- (b) Where non-Internet based communication of alerts is required (e.g., to radio-controlled sirens or other dissemination systems, or where non-standard or proprietary interfaces must be supported) such communication can be implemented using external adaptors that interface to the CAP Server in accordance with these requirements.
- (c) The CAP Server interface for alert submission is implemented using an HTTP POST from the source to the CAP Server using basic HTTP authentication. The message body is the CAP XML message.

- (d) The CAP Server interface for general alert publication is by direct HTTP retrieval of individual CAP XML documents from the CAP Server, facilitated by an HTTP readable index of all unexpired public messages in the Atom Syndication Format. The index and the individual CAP alert files are readable by any individual or system on the Internet. The format of the index file is described in the section **“CAP and Atom File Formatting”** below.
- (e) The CAP Server interface for directed alert forwarding is implemented using an HTTP POST from the CAP Server to the target system using basic HTTP authentication. The message body is the CAP XML message.
- (f) In the event of a failed initial transmission by the CAP Server directed forwarding interface to a particular recipient (as indicated by receipt of any HTTP status code other than 200, 201 or 202, or of no HTTP status code) the CAP Server shall attempt to retry delivery to that recipient at ten second intervals for the first three minutes, then at twenty second intervals for the next five minutes, then at thirty second intervals for so long as the message remains unexpired.

3. CAP AND ATOM FILE FORMATTING

- (a) CAP alerts generated by the CAP Server describe the affected area by using the geospatial CAP **polygon and circle elements as well as defined geocode values to define alerting zone definitions. This list is given in the Table “Community Geocodes” below and can be expanded at any time using the Administration interface to define new alerting zone definitions.**
- (b) CAP messages containing sensor or other operational data not intended for public dissemination is identified by populating the CAP **scope** element with a value of “Private.” Such messages are NOT included in the general publication Atom index.
- (c) CAP messages containing technical information about alerting device or system status or errors are identified by populating the CAP **status** element with the value of “System.” Such messages are NOT included in the general publication Atom index.
- (d) The Atom-formatted index **entry** block for each alert on the CAP Server publication interface includes the following elements:
 - i. The Atom **link** element include the URL of the corresponding CAP XML file in the **href** attribute.
 - ii. The Atom **title** element contain the value of the CAP message’s **headline** element.
 - iii. The Atom **updated** element contain the value of the CAP message’s **sent** element. \
 - iv. The following CAP elements are included in the Atom file with a namespace prefix of “cap” (which prefix is bound in the XML preamble to the OASIS CAP 1.2 namespace):
 - A. status
 - B. msgType
 - C. language

- D. category
- E. urgency
- F. severity
- G. certainty
- H. areaDesc
- I. geocode

- (e) In the case of CAP messages containing an **expires** element, the message is considered unexpired until after the latest **expires** time in any included CAP **info** block. If no **expires** element is present in a CAP message that message is considered unexpired until one hour after its **sent** time value.

4. CUSTOM PARAMETERS

Inevitably in any pre-existing warning system there will be legacy components to be supported or existing desired functionality to be retained requiring the use of <parameter> values. The following CAP parameter values must be supported by the CAP server for this application.

Inhibit Parameter

Inhibit Parameter Description and Methodology

The inhibit parameter is included to provide the utmost granularity of alert dissemination methods to be activated for a particular alert. The presence of a “TRUE” inhibit parameter in an alert for a particular dissemination mechanism means that mechanism will NOT activate regardless of any other activation criteria being met. The absence of an inhibit parameter or a value of false indicates that the dissemination method will determine its activation based on its filters, i.e. normal operation.

Structure

The inhibit tag is a parameter value in CAP.

Format :

```
<Parameter>
<Valuename>inhibit-AlertMechanismName </Valuename>
<Value>True / False <Value>
</Parameter>
```

Where AlertMechanismName is a unique predefined string for each alert dissemination method. All dissemination methods attached to the system will be assigned an AlertMechanismName and a “Friendly name” (FriendlyName) which is to be displayed in the GUI of the Administration and Activation interfaces. Refer to the section entitled “GUI Guidelines” below.

Implementation

The inhibit tag will be implemented on the CAP server as follows:

On the Administration and Activation interfaces it will be implemented as a checkbox for each defined alert mechanism. There will be a minimum of twelve (12) checkboxes available for this purpose.

As new mechanisms are added to the system their corresponding AlertMechanismName and FriendlyNames can be added under the Administration interface. Once these are added an additional checkbox labeled with the “Friendly Name” will be added to both the Administration and Activation interfaces for each new alert and alert template.

By default each checkbox is “checked”. A value of checked corresponds to an inhibit parameter value of **False**. An inhibit value of False is an optional parameter in the CAP XML as its absence is also interpreted as a False Value. A value of unchecked or cleared indicates that the inhibit value for that alert mechanism should be set to **True**. **inhibit parameter values that are set to True MUST be included in the CAP XML**. . Refer to the section entitled “GUI Guidelines” below

Several dissemination methods already have their AlertMechanismName and FriendlyName defined. Please refer to the table below.

Alert Method	FriendlyName	AlertMechanismName
Cable TV	Cable TV Interrupt	tv
FM Broadcast Interrupt	FM Radio Interrupt	radio
Marine Alert	Marine Radio	marine
Weather Radio	Weather Radio	weather
Email Server	Email	email
RDS receivers	RDS receivers	rds
Smartphone app	Smartphones	smartphone
Sirens	Sirens	siren
SMS	SMS Text Message	sms

5. SECURITY, AUTHENTICATION AND AUDITING

- (a) All Internet connections utilized by the CAP Server interfaces are encrypted using Transport Layer Security (TLS) version 1.0

- (b) All Internet connections utilized by the CAP Server submission and directed forwarding interfaces are authenticated using an identifier and password which uniquely identifies the source device or system.
- (c) In the case of a message received from a human originator, the identifier uniquely identify the individual responsible for the message content.
- (d) To ensure accountability, The CAP Server shall apply an XML Digital Signature as described in the OASIS CAP 1.2 specification to each new CAP alert it receives from an authorized local originator. Digitally signed messages may be verified at any time or location thereafter to ensure that they have not been distorted or modified since they were originated.
- (e) The CAP Server shall publish the public key it uses for signing alert messages as an X.509 formatted digital certificate accessible at an Internet URL. The CAP Server also publish all previously used certificates and a certificate revocation list in accordance with ITU-T recommendation X.509.
- (f) The CAP Server shall attempt to verify each received CAP alert that contains a digital signature, and offer configuration options in its Administration interface to reject:
 - i. Unsigned CAP alerts; and/or,
 - ii. Signed CAP alerts that fail verification.
- (g) The CAP Server maintain a complete auditable record of all:
 - i. Alerts received, published or routed;
 - ii. Accesses to the web interfaces for user authentication, alert processing policies, alert zones, message templates and other administrative actions;
 - iii. System errors including authentication and digital signature verification failures and errors from the underlying operating software and/or hardware; and,
 - iv. Email subscriptions and subscription cancellations, including automatic cancellations.
- (h) All such records are maintained within the CAP Server for the preceding twelve months, and a method shall be provided for transferring older records to external archival storage.

6. WEB ALERT ORIGATION SUBSYSTEM

- (a) The CAP Server shall provide a web-based mechanism by which authorized user may issue alerts from any standard web browser, including a version of the interface suitable for web browsers on Blackberry and other “smartphone” devices.
- (b) The web alert origination interface enable an authenticated and authorized alert originator to :

- i. Select from alerting zones previously configured on the CAP server.
 - ii. Select and edit alert templates previously configured on the CAP server. (An alert template includes the message template as well as the selection of dissemination methods.)
 - iii. Select and edit alerts received via the API that are not configured for automatic submission. (see section Application Programming Interface)
 - iv. Select and add up to two (2) multimedia files to attach to the alert using resource.uri tags. Please see section entitled MultiMedia Formats below for specifications.
 - v. Review and revise the alert prior to release.
 - vi. Save the alert as a new alerting template if desired (changes made to templates that have been predefined on the Administration interface are not persistent).
- (c) Changes to alert templates under the web alert subsystem are not persistent and are effective only for the current alert instance.
- (d) The web alert origination interface shall require manual entry of a valid individual user identifier and password previously established through the authentication control interface on the CAP Server.

7. APPLICATION PROGRAMMING INTERFACE (API)

- (a) The CAP server shall provide a web based API to allow automatic submission of CAP alerts by devices such as Weather Stations, Rain Gauges etc.
- (b) The API for alert submission is implemented using an HTTP POST from the source to the CAP Server using basic HTTP authentication. The message body is the CAP XML message. Multimedia submission (images and audio) to be attached to the alert will be also be submitted via this interface.
- (c) All messages sent via the API directly (not using the web alert origination interface) MUST be SIGNED using the X.509 formatted digital certificate from the CAP server. Unsigned messages will be logged but disregarded. The API will provide the appropriate status message indicating the failure.
- (d) The API will implement all necessary security measures to prevent abuse including measures to deal with repeated unsuccessful authentication attempts.
- (e) The web server must provide a method of classifying alerts received via the API as requiring manual activation or being automatically dispatched on receipt. This setting must be available for each authorized alert submitting device and is defined by Administrators for all alerts received from that device.

8. ELECTRONIC MAIL NOTIFICATION SUBSYSTEM

- (a) The CAP Server shall provide a web-based mechanism by which members of the public may subscribe or unsubscribe Internet email addresses for automatic notification of new alerts.
- (b) Email alerts include at a minimum all CAP **sender, sent, source, headline, description**, certainty, severity, urgency, **instruction, web, resource.uri** and **areaDesc** values.
- (c) On subscription the user will be allowed to select the preferred language for alert. The CAP server will deliver CAP messages with the corresponding language code to the user in addition to all messages sent in English.
- (d) Upon subscription or cancellation of an email address through the web interface specified above, a confirmation email is sent to the email address in question, and no further action is taken until an affirmative response to that email has been received.
- (e) The email notification subsystem monitors email delivery failure notifications (“bounce messages”) and automatically unsubscribe any address for which it receives failure notifications for five alerts in sequence.
- (f) The email server must support the inhibit parameter as described in the section Custom Parameters. The **AlertMechanismName for the email server is: email. The FriendlyName is : Email**
- (g) The email notification subsystem of the CAP Server shall implement an internal SMTP Mail Transfer Agent (MTA).
- (h) Any emails not yet forwarded by the MTA when the subject alert expires (either at the latest CAP **expires** time or, if no **expires** element is present, one hour after the CAP **sent** time) is purged from the outgoing mail queue and an email delivery failure is recorded for that recipient.
- (i) The Email server is a self-contained module of the CAP server and will reside on the same hardware. It will not require any additional resources beyond the specifications of the CAP server.
- (j) The technical specifications for the email server also include those specified in the section entitled “General specifications for alert dissemination devices” contained herein.

9. SMARTPHONE APPLICATION

A smartphone application compatible with the following two Smartphone Operating Systems shall be provided. (Android and iOS). The application must be able to poll for and deliver notification of warnings even when it is not in the active or foreground frame. This may require the use of a background daemon to continue to poll for alerts when the application is closed or employ the appropriate PUSH features of the operating system in order to achieve the same effect. The application is considered an alert dissemination method and thereby must meet all the requirements of alert dissemination methods including support of the inhibit parameter.

Application features

- (a) The application must be able to poll both CAP servers for alerts.

- (b) The application must be able to poll servers in a background process or employ PUSH notifications to allow notification of alerts when the application is not in the foreground or active state.
- (c) When an alert is received the application will notify the user via user selectable mechanisms which may include “pop ups”, vibration, ringtones and notification lights.
- (d) The application must provide a list of all unexpired alerts for users to view. The following CAP fields are the minimum that shall be displayed for each such alert: **sender, sent, source, headline, description, instruction, web, certainty, severity, urgency resource.uri** and **areaDesc**.
- (e) The application must also provide for viewing expired alerts for the last seven (7) days.
- (f) The application must support the inhibit parameter as described in the section Custom Parameters. The **AlertMechanismName for the application is: smartphone. The FriendlyName is : smartphones**
- (g) The Smartphone module is a self-contained module of the CAP server and will reside on the same hardware. It will not require any additional resources beyond the specifications of the CAP server.
- (h) The technical specifications for the Smartphone module also include those specified in the section entitled “General specifications for alert dissemination devices” contained herein.

10. GUI GUIDELINES

This section provides more detailed information on the expected look of the network interfaces for the CAP server. Some prototyping diagrams are also included to support a design that is consistent with the existing system and is intended to minimize retraining costs and effort.

Guidelines for web alert origination subsystem.

Generally the UI should be simple and uncluttered. Use of proprietary softwares and plugins such as Adobe Flash, Microsoft Silverlight etc are NOT encouraged. In order to ensure maximum support by browsers and computing devices the following general observations are to be made:

- (a) There shall be no use of proprietary web technologies and plugins e.g. Adobe Flash and Microsoft Silverlight (Javascript, HTML5, CSS however may be used).
- (b) The UI should be spread across a small number of pages to avoid clutter and make provisions for small screens.
 - The prototyping images in this section are a suggested layout. This layout preserves most of the elements of and hence familiarity with the legacy system minimizing retraining costs and effort.
 - Each image is followed by a table listing and describing the elements contained herein. Suggested element types are standard HTML5 elements.

Alert Creation Page 1 of 3

Anguilla Warning System

Logged in as : Director
 DDM

Tuesday 02nd february 2014 9:00 AM

Hurricane

↓

1. Alert Template

Affected Areas

☐ ISLANDWIDE
 ☐ DisasterZone 1
 ☐ Disaster Zone 2
 ☐ Disaster Zone 3
 ☐ Disaster Zone 4

DisasterZone1 : Island Harbour , East End

DisasterZone2 : Sandy Hill , Long path, Little Dix, Valley Central

DisasterZone3 : Blowing Point , George Hill, South Hill

DisasterZone 4 : West end , Meads Bay, Long Bay

* Please note that it is better to error on the side of caution. it is advisable to select too many areas of impact than too little

LOGOUT

NEXT

Element Description / Label	Element Type	Purpose / Notes
Logged in as	Non editable text field	Shows current user logged into system
Date & Time	Non editable text field	System Date and Time
1. Alert template	Drop Down box	Select Alert template
LOGOUT	Button	Log out of server

NEXT	Button	Proceed to next step in alert creation
------	--------	--

Alert Creation Page 2 of 3

Anguilla Warning System

Logged in as : Director
DDM

Tuesday 02nd february 2014 9:00 AM

Hurricane

Language English

Expected Duration 15 minutes

Status	Certainty	Severity	Urgency
☒ Actual	Observed	☒ Extreme	☒ Immediate
Exercise	Likely	Severe	Expected
Test	☒ Possible	Moderate	Future
Draft	Unlikely	Minor	Past
System	Unknown	Unknown	Unknown

ALLOW ACTIVATION OF :

☐ FM Radio Interrupt
 ☐ Blackberry App
 ☐ Email
 ☐ Marine Radio
 ☐ Sirens
 ☐ RDS Receivers
 ☐ Weather Radio
 ☐ Smartphones

LOGOUT
BACK
SAVE AS NEW TEMPLATE
NEXT

Element Description / Label	Element Type	Purpose / Notes
Logged in as	Non editable text field	Shows current user logged into system
Date & Time	Non editable text field	System Date and Time
Event Code	Drop Down box	Event Code (CAP category element)
Language	Drop Down box	Alert dissemination language (CAP language element)
Expected Duration	Drop Down box	Sets time before alert expires (CAP expires element)
Status	Slider	CAP Status element
Certainty / Severity /Urgency	Slider	Sets corresponding CAP values
ALLOW ACTIVATION OF:	Checkbox Array	These checkboxes directly correspond to the inhibit tag as described in the section entitled “Custom parameters” above. The number of checkboxes displayed directly correspond to the number of AlertDisseminationNames (dissemination methods) defined in the Administration interface. As part of the alert template changes to these values are not persistent across sessions.
LOGOUT	Button	Log out of server
BACK	Button	Return to previous step in alert creation (maintaining any changes made)
SAVE AS NEW TEMPLATE	Button	As a result of the fact that changes in the web alert dissemination interface to any alert template predefined in the Administration interface are not

		persistent the option to save the currently modified alert as a new alert template is provided.
NEXT	Button	Proceed to next step in alert creation

Anguilla Warning System

Logged in as : Director
DDM

Tuesday 02nd february 2014 9:00 AM

Hurricane

Authorised source of message

Alert Summary (160 characters maximum)

Event Description

Instructions

Contact

Sent by

Add Multimedia to alert

Add File

Add File

SEND ALERT

LOGOUT

BACK

SAVE AS NEW TEMPLATE

PREVIEW

Element Description / Label	Element Type	Purpose / Notes
Logged in as	Non editable text field	Shows current user logged into system
Date & Time	Non editable text field	System Date and Time
Authorized source of message	Text field	Name of person or agency that authorized the sending of the alert. Corresponds to CAP element : sender
Status	Slider	CAP Status element
Alert Summary	Text box (limited to 160 characters)	A single line summarizing the event causing the alert. The maximum length of 160 characters must be enforced. Corresponds to CAP element : headline
Event Description	Multi line text field	The full textual description of the situation. Corresponds to CAP element : description
Instructions	Multi line text field	Instructions for the public to follow in response to alert. Corresponds to CAP element : instructions
Contact	Multi line text field	Contact information. Corresponds to CAP element : contact
Sent by	Text field	The name / position of the person activating the alert. Corresponds to CAP element : senderName
Add File	Button , textbox , Button	This interface is used to add multimedia to the alert (refer to section entitled MultiMedia Formats). Clicking “Add File” button with the corresponding text field empty indicates that the user

		wishes to select a file from the local system to upload. A progress indicator must be displayed for the upload process. A facility to cancel the upload at any time must be provided After the upload the corresponding text field must be updated with the fully qualified HTML link to the uploaded file on the CAP server and the HTML link to the uploaded file included in a resource.uri tag in the CAP alert. Clicking “Add File” button with a fully qualified HTML link already in the corresponding text field incorporates the HTML link in a resource.uri tag in the CAP alert. Clicking the red x will clear the corresponding text field and remove the corresponding resource.uri tag from the CAP file
Preview	Button	Gives a preview of the raw CAP of the alert
SEND ALERT	Button	Submits alert for activation as described in section web alert origination subsystem
LOGOUT	Button	Log out of server
BACK	Button	Return to previous step in alert creation (maintaining any changes made)
SAVE AS NEW TEMPLATE	Button	As a result of the fact that changes in the web alert dissemination interface to any alert template predefined in the Administration interface are not

		persistent the option to save the currently modified alert as a new alert template is provided. This modified template will only be available to the user that created it.
NEXT	Button	Proceed to next step in alert creation

11. MULTIMEDIA FORMATS

The CAP server shall allow the attachment of the following media types to any alert template.

Images : PNG, BMP, JPG, GIF

Audio : MP3, WAV

Video : AVI, MP4, MPEG

- (a) When multimedia is uploaded from a remote source (i.e. a file from the local machine of the activator) the media is uploaded to the CAP Server and made available via HTML link
- (b) The HTML link shall be encapsulated in the CAP resource element (uri) along with the corresponding MIME type
- (c) Multimedia is purged from the system according to the same schedule as old CAP alerts or as necessary if the CAP server needs storage space on a least recently created basis.
- (d) When multimedia is uploaded from a remote source the following file size limits are enforced :

Images : 1.5 MB

Audio : 3 MB

Video : 4 MB

- (e) Attempts to upload any file that does not meet the specifications contained herein shall result in an error and a notification to the user of the file's incompatibility.

12. SYSTEM PERFORMANCE

- (a) The CAP Server is capable of performing the following alert processing sequence within ten (10) seconds of either the first communication with the CAP message submission interface (API) or release of the message via the web interface:
 - i. Authenticate the alert source
 - ii. Accept an alert message in either CAP or HTML form format and return the appropriate HTML acknowledgement to the source;
 - iii. If in CAP format and digitally signed, verify the digital signature
 - iv. If submitted by the web interface or API, convert to CAP format with digital signature;
 - v. If the alert is Public and Actual, update the publication interface Atom index and make the message retrievable by HTML request;
 - vi. Compare the alert to the forwarding policies for up to ten directed-forwarding recipients and make a first attempt to deliver to all eligible recipients via the directed-forwarding interface;
 - vii. Query a current database of up to 20,000 email subscriptions and prepare and queue to the MTA up to 20,000 emails and,
 - viii. Make log entries as appropriate.
- (b) The CAP Server is capable of maintaining the above performance standard at an incoming message rate of one alert every ten seconds sustained for a period of at least one hour.
- (c) The hardware and software for The CAP Server is designed to maintain the above levels of complete system performance in continuous operation with no more than the following unscheduled downtime:
 - i. Ten seconds total per day;
 - ii. Five minutes total per month; or,
 - iii. One hour total per year.
- (d) The hardware and software for each local CAP server is designed to work with one (1) Public Static IP address linked to a single domain name as provided by the receiving agency.
- (e) The secondary CAP servers are Virtual Machines on a physical server located outside of the region. The domain names for the secondary servers are to be the same as the local servers with only a minimal change in the URL to specify the Secondary server as opposed to the Primary server.

- (f) The hardware for The CAP Server shall include an Uninterruptable Power Supply (UPS) of sufficient capacity to sustain the CAP Server for at least twelve (12) hours in the absence of mains power. The UPS shall signal the CAP Server if it approaches exhaustion, and the CAP Server shall automatically shut down upon receiving such a signal. The CAP Server shall automatically restart when power is restored.

13. GENERAL SPECIFICATIONS FOR ALERT DISSEMINATION DEVICES

All alert dissemination devices connected to the CAP server have the following general technical specifications.

- (a) Devices receive CAP v 1.2 alerts by “POLLING” the CAP servers and processing the atom file containing the list and URI’s of active alerts.
- (b) Devices will process unique CAP messages and disregard any identical duplicated alerts which may be received from multiple CAP server sources.
- (c) Devices must be able to poll a list of at least two (2) CAP servers for active alerts at least once every sixty (60) seconds. Where an alternate polling interval is required the individual technical specifications will indicate this.
- (d) Devices will be designed to use a dynamic IP address (such as common with ADSL internet service) and must include self-contained Dynamic DNS clients.
- (e) Devices will be designed to utilise standard ADSL internet access with standard RJ45 interfaces.
- (f) Devices will keep a completely auditable log of all alerts received, disseminated and disregarded.
- (g) Devices will be fully compatible with the requirements set out in the section titled “CUSTOM PARAMETERS” in this document.
- (h) Devices will feature a web interface accessible from the internet (with appropriate security and authentication) from which all dissemination options can be configured.
- (i) Devices will implement all necessary self-diagnostic and internet connectivity status tests and a reporting facility via an HTTP “GET” or “POST” mechanism of device status. A HTTP response of “OK” indicating normal function and “FAIL – xxxxxx” where xxx is an error code defined in user documentation or a textual description of an error condition if a malfunction or otherwise unexpected condition arises.

14. DOCUMENTATION AND LICENSES

Upon delivery of each CAP server the local receiving agency shall be provided:

- i. Complete operator's and system administrator's instruction manuals (in hard and electronic copy) for the system;
- ii. A legally valid and binding document conveying clear title to all system hardware to the receiving agency;
- iii. A legally valid and binding document granting an irrevocable unlimited term license for use of all software provided as part of the system, and for unlimited use of updated, enhanced or derived versions of such software; and,
- iv. One copy of each manual, license, warranty and safety document provided by the original manufacture with any component of the control system.

15. DELIVERY, INSTALLATION AND ACCEPTANCE TESTING

- (a) Within 20 days of award of contract the selected provider shall submit to UNDP a list of any additional requirements for physical, electrical and network site preparations required for installation of the CAP server for each country.
- (b) Within 30 days of award of contract the selected provider shall submit to UNDP a detailed test procedure that is designed to completely test, verify and illustrate the CAP server's compliance with the requirements in this document for approval by UNDP.
- (c) Within 30 days of receiving written notification from UNDP that one or more sites are ready for installation the selected provider shall :
 - i. Deliver all components of the CAP server to the specified location;
 - ii. Install all components of the CAP server including making all mechanical, electrical and network connections required for its function;
 - iii. Conduct an acceptance test procedure that completely demonstrates each CAP server's compliance with the requirements set forth above;
 - iv. Provide a written report documenting the design of the above testing, the date of its performance, the results of the testing and certifying the report as accurate and complete;
 - v. Provide the receiving local agency with all documents as specified in the section above and,
 - vi. Provide the receiving local agency with a draft Letter of Acceptance by which the local agency may accept custody and ownership of the provided equipment and software.

- (d) The selected provider shall obtain all transportation services, storage services, customs clearances and any other permits or services required to deliver, install and test each locally installed or Primary CAP server. The safety and security of all equipment shall be the sole responsibility of the selected provider until installation and testing are complete and the local receiving agency has taken custody in writing.
- (e) The selected provider shall secure all necessary insurance and work permits and shall perform all other acts required by each local jurisdiction for the employment of staff. Sub-contractors and local employees engaged in the delivery, installation and testing processes.

16. HARDWARE AND SOFTWARE SUITABILITY

- (a) All equipment and software for each CAP server shall meet or exceed all electrical, environmental, safety and other suitability standards for ICT systems in force at the place and time of its installation.

17. WARRANTIES AND MAINTENANCE

- (a) The selected provider shall provide maintenance for each CAP server as described below for a period of three (3) years after operational handover ("the maintenance period") at no additional cost.
- (b) Throughout the maintenance period the selected provider shall maintain a point of contact by post, email and telephone through which the local agency responsible for each CAP server can request service during business hours.
- (c) During the first ninety (90) days after transfer of custody of each CAP server the selected provider shall, during business hours at its usual business location, provide up to ten hours of telephone software support to each local responsible agency or to another agency or contractor designated by the responsible agency.
- (d) Throughout the maintenance period the selected provider shall provide, at no cost, online software updates to the operating system and all other software, including recommendation operating system updates and application patches. Such maintenance shall be coordinated in advance with the local agency responsible for the CAP server.
- (e) Software updates that change the operating procedures or interfaces for the CAP server shall NOT be deployed without one week's advance notice to each operating agency and shall NOT be applied to any CAP server until approved by its responsible agency.

18. OPEN SOURCE PREFERENCES

- (a) Preference will be shown to proposals that utilise operating system and other software that is published under an open source license approved by the Open Source Initiative. (www.opensource.org).
- (b) Additional preference will be shown to proposals that generate new software that will be published under an open source license approved by the Open Source Initiative (www.opensource.org) at the time the first CAP system is delivered.