

# National Alert Aggregation & Dissemination System

---

## Last Mile Distributor - User Guide

Release 7.0a



2655 Bristol Circle  
Oakville, Ontario L6H 7W1  
T 905 829.1159  
F 905 829.5800

**Pelmorex Communications Inc.**

2655 Bristol Circle,  
Oakville, Ontario L6H 7W1  
T 905 829.1159  
F 905 829.5800

Copyright © 2015 Pelmorex Communications Inc. All rights reserved.

This document was last updated on: 03/30/2015.

All other product names and trade names used herein are trademarks of their respective owners. Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of Pelmorex Communications Inc.

## Table of Contents

|   |           |
|---|-----------|
| <b>Welcome!</b>   | <b>5</b>  |
| Overview  | 5         |
| NAAD Service Desk   | 5         |
| Who Should Use this Guide?                                    | 5         |
| Symbols Used in this Guide                                    | 5         |
| Acronyms  | 5         |
| <b>TERMS AND CONDITIONS OF USE</b>                            | <b>7</b>  |
| <b>NAAD System - Overview</b>                                 | <b>8</b>  |
| About this chapter  | 8         |
| NAAD System Introduction                                      | 8         |
| Information for LMDs  | 9         |
| General Rules/Concepts  | 9         |
| 5 MB Alert Size   | 10        |
| Trusted Feed – EC Alerts                                      | 10        |
| Multiple Info-Blocks  | 10        |
| Rules for attachments   | 11        |
| Display of special characters for LMDs                        | 11        |
| Rules Governing NAAD System Testing & Test Messages           | 12        |
| Sections to follow  | 12        |
| Reference Documents   | 12        |
| User Resources  | 12        |
| <b>Chapter 2</b>  | <b>14</b> |
| <b>NAAD System Feed Specifications</b>                        | <b>14</b> |
| About NAAD System Feeds                                       | 14        |
| Satellite and TCP Streaming Feed – General Information        | 14        |
| 1. Satellite Feed   | 15        |
| Summary and additional notes for the Satellite Feed           | 16        |
| 2. Internet TCP Streaming Feed                                | 16        |
| Summary and additional notes for the TCP Streaming Feed       | 17        |
| 3. Internet GeoRSS Feed                                       | 18        |
| Summary and additional notes for the GeoRSS Feed              | 18        |
| 4. Troubleshooting Internet TCP Streaming Feed                | 19        |
| <b>Chapter 3</b>  | <b>20</b> |
| <b>Satellite Dissemination</b>                                | <b>20</b> |
| About Satellite Dissemination                                 | 20        |
| 1. Satellite Dissemination – C Band                           | 20        |
| 2. Satellite Dissemination – Ku Band                          | 21        |
| ADDENDUM A – C Band   | 22        |
| EXAMPLE A: CONFIGURING CISCO D-9850 RECEIVER (PRIMARY FEED)   | 23        |
| EXAMPLE B: CONFIGURING CISCO D-9850 RECEIVER (SECONDARY FEED) | 26        |
| ADDENDUM B – Ku Band  | 28        |
| <b>Appendix 1: Heartbeats</b>                                 | <b>29</b> |
| <b>Appendix 2: Sample Alert Messages</b>                      | <b>31</b> |
| <b>Appendix 3: Broadcast Intrusive Alerts</b>                 | <b>36</b> |
| <b>Broadcast Intrusive SOREM List</b>                         | <b>38</b> |
| <b>Appendix 4: Digital Signatures</b>                         | <b>40</b> |
| <b>Appendix 5: Sample EC Alert</b>                            | <b>49</b> |

## Table of Figures

|  |    |
|--|----|
| Figure 1 – Satellite Dissemination – C Band.....   | 21 |
| Figure 2 – Satellite Dissemination – Ku Band ..... | 22 |

## Welcome!

This document provides information and describes the features of the **National Alert Aggregation & Dissemination (NAAD)** System provided by Pelmorex Communications Inc ("Pelmorex"). It is intended to assist Last Mile Distributors (LMD) so LMDs can receive and pass on Alert Messages to the public.

## Overview

The NAAD System collects public alert messages from Authorized Government Agencies (AGA) and makes them available (without any alteration or interpretation of the contents) to LMDs such as radio and television stations, as well as cable and satellite TV companies for display to the Canadian public thereby helping forewarn the public of any imminent danger related to persons or property. This User Manual will provide the information necessary for interested LMDs to effectively monitor Alert Messages disseminated over the NAAD System.

## NAAD Service Desk





The Service Desk is the Single Point of Contact for all NAAD System users. The Service Desk analyst can be reached at [Support-PublicAlerting@Pelmorex.com](mailto:Support-PublicAlerting@Pelmorex.com).

## Who Should Use this Guide?

Participating LMDs or those who are interested in participating in receiving alerts from the NAAD System should read this guide.

## Symbols Used in this Guide

Look for the following symbols as you read through this guide, for further assistance:

| Symbol  | Description   |
|---|---|
|  | <b>Note</b><br>Calls your attention to additional information.                        |
|  | <b>Tip</b><br>Calls your attention to a useful tip.                                   |
|  | <b>Warning</b><br>Calls your attention to an important warning.                       |
|  | <b>New Feature</b><br>Calls your attention to features introduced in the new release. |

## Acronyms

|                 |   |
|-----------------|---|
| <b>AGA</b>      | Authorized Government Agencies              |
| <b>CAP</b>      | Common Alerting Protocol                    |
| <b>CAP - CP</b> | Common Alerting Protocol - Canadian Profile |

|                    |   |
|--------------------|---|
| <b>HTML</b>        | Hyper Text Markup Language                        |
| <b>LMD</b>         | Last Mile Distributors                            |
| <b>LNB</b>         | Low Noise Block down converter                    |
| <b>NAAD System</b> | National Alert Aggregation & Dissemination System |
| <b>TCP</b>         | Transmission Control Protocol                     |
| <b>URL</b>         | Uniform Resource Locator                          |
| <b>XML</b>         | Extensible Markup Language                        |
| <b>EC</b>          | Environment Canada                                |

## TERMS AND CONDITIONS OF USE

By using the National Alert Aggregation and Dissemination ("NAAD") System Alerting Data Feed, you agree to accept and abide by these Terms and Conditions of Use. You further acknowledge and agree that Pelmorex Communications Inc. ("Pelmorex") may revise and update these Terms and Conditions of Use without notice to you at any time.

All alerts, content, material and information (hereafter "emergency information") provided on the NAAD System Alerting Data Feed is obtained by Pelmorex from a government agency in Canada that is authorized to issue emergency information and is provided on an "as is" basis.

Pelmorex makes every reasonable effort to ensure the NAAD System Alerting Data Feed contains only emergency information received from a government agency in Canada that is authorized to issue emergency warnings and that the public safety messages comply with agreed to standards as posted elsewhere on Pelmorex's website at <https://alerts.pelmorex.com/>. However, Pelmorex does not guarantee, or make any representation or warranty, express or implied, (i) that the messages contained in the emergency information are current, accurate, truthful or complete; or (ii) that the emergency information will be available without interruption, error or omission.

Under no circumstances, including, but not limited to, negligence, gross negligence, negligent misrepresentation and fundamental breach, shall Pelmorex or its affiliates and related companies, and each of their respective directors, officers, employees, consultants and agents be liable for any direct, indirect, incidental, special or consequential damages or any loss that results from the use of, or the failure to use, any emergency information, or postings on the NAAD System Alerting Data Feed, directly or indirectly. These limitations apply regardless of whether the party liable or allegedly liable was advised, had other reason to know, or in fact knew of the possibility of such damages.

Further, in viewing the NAAD System Alerting Data Feed, you specifically acknowledge and agree that neither Pelmorex nor its affiliates and related companies, nor each of their respective directors, officers, employees, consultants and agents shall be liable for any defamatory, offensive or illegal conduct of any user, including you.

## Chapter 1

# NAAD System - Overview

This chapter includes...

- NAAD System Introduction
- Information for LMDs
- General Rules/Concepts
- Rules for attachments
- Display of special characters for LMDs
- Rules Governing NAAD System Testing & Test Messages
- Sections to follow
- Reference Documents
- User Resources

## About this chapter

The aim of this chapter is to provide the basic concept and information about the NAAD System and Alert Messages issued through the NAAD System, and to give an overview of the Alert Message rules (rules refer to the CAP/CAP-CP standards and policies adopted by the Council) to the LMDs.

## NAAD System Introduction

The NAAD System provides 3 basic features as described below:

### 1. Collection of Alert Messages

The NAAD System provides the ability for AGAs to create Alert Messages or issue alerts through a trusted feed if an organization has a public alerting system (as in the case of Alberta and EC). Therefore, Alert Messages can be sourced from:

- The 'User Access System' provided by the NAAD System (Issuers create alerts which are then submitted for dissemination to LMDs),
- As Trusted Feeds; where Alert Messages are received from an AGA's system as a data feed already assembled and validated (by the issuing AGA) as CAP-CP compliant.

### 2. Aggregation of Alert Messages

Aggregation of Alert Messages implies the aggregation of alert messages submitted by the AGAs (the participating sources for sending alerts in Canada). Information is collected/stored, processed and validated against CAP-CP standards, permissions/authorizations and agreed upon rules. The basic steps are:

- Validate the alert message format & authority,
- Merge all sources,
- Log, record & archive Alert Messages.



The NAAD System does not aggregate certain elements of an alert, for instance the attachments referenced by URL.



### 3. Dissemination of Alert Messages

Dissemination of alert messages implies making the Alert Message available to various LMDs for further dissemination to the general public.

Alert Messages are disseminated to LMDs in the following manner:

- via real-time streaming feeds for 24/7 automated system implementations,
- through an auxiliary repository as well as GeoRSS feed for occasional access.

### Information for LMDs

To receive Alert Messages for dissemination to the general public, an LMD should be aware of the basic rules/concepts of the NAAD System set out below.

- Multiple feeds are made available; it is recommended that LMDs listen to more than one feed for redundancy purposes.
- Use CAP & CAP-CP standard to interpret, select and publish the Alert Messages. Alerts contain all the information for the LMD to filter, interpret, profile as needed by their own network.
- Use Digital Signatures to verify that Alert Messages are from a genuine source; Alerts contain 1 or 2 Digital Signature(s); it is recommended that LMDs verify signatures to ensure the message is from a genuine AGA as well as received via the NAAD System.
- Use auxiliary mechanisms to retrieve Alert Messages if message loss is detected. Messages are kept in their integral form for 48 hours (short term repository) for automated retrieval if an alert was missed by a LMD.
- Know the concept of Heartbeats; Heartbeats let an LMD know that the NAAD System is operating properly and provides information about previous Alert Messages.



More detail on all of the above mentioned points is provided in the subsequent chapters.

### General Rules/Concepts

An LMD should be aware of the following rules and concepts governing Alert Messages:

- All Alert Messages follow the CAP/CAP-CP approved standards.
- All Alert Messages have certain Business rules as well such as limits on message sizes, attachment sizes and types, mandatory expiry, language codes etc. For details refer to the [technical information section](https://alerts.pelmorex.com/) at <https://alerts.pelmorex.com/>.
- The NAAD System streams Alert Messages in CAP format as they are received.
- The NAAD System may repeat transmission of an Alert Message only if a transmission error has been detected on a specific stream; transmission is only repeated on the data stream containing the error.
- The NAAD System does not filter, interpret or change the content of the Alert Messages (a Digital Signature is added by Pelmorex to each Alert Message to validate its authenticity).
- A specific Alert Message received on a system stream (C band, Ku Band or TCP feeds) or accessed from the short term retrieval repository is identical byte for byte regardless of the medium from which it was obtained.

- A NAAD System Heartbeat message is sent regularly (every 60 seconds) to provide LMDs with the capability to monitor that the feed is 'live' as well as to detect the loss of an Alert Message.
- The Heartbeat message:
  - Contains a list of the latest (10) transmitted Alert Messages,
  - Is not digitally signed,
  - Is compliant with CAP-CP standards.
- A GeoRSS link is provided by the NAAD System to allow users to manually see in their native i.e. in XML form the Alert Messages issued in the last 48 hours.
- The NAAD System also provides:
  - A short term repository (up to the last 48 hrs.) where alerts missed by a LMD can be retrieved,
  - A user "archive" site where all Alert Messages are kept.
- LMDs should listen to more than one feed for redundancy purposes; these can be C Band, Ku Band or TCP Streaming or a combination of these feeds.
- The NAAD System will support only the following 3rd language coding: (over and above the two official languages)

| Third Language | Language Code |
|----------------|---------------|
| Cree           | cr            |
| Dene           | chp           |
| Inuinnaqtun    | ikt           |
| Inuktitut      | iu            |

## 5 MB Alert Size

In June 2010 when the NAAD System first launched the maximum size of an alert was limited to 1 MB. This limit has been changed & increased to 5 MB in NAADS Release R4.0. The system supports the size of 5 MB per alert.

## Trusted Feed – EC Alerts

The NAAD System also supports a Trusted Feed from Environment Canada (EC) and EC alerts are available on the NAAD System feeds/outputs in addition to alerts issued through the NAAD System Issuer Interface.

An LMD can identify EC alerts by the [the <source> tag in the CAP XML](#). For example, EC alerts will contain the following [<source>Environment Canada - Environnement Canada - Toronto \(CWTO\)</source>](#). See Appendix 5 for a Sample EC Alert.

## Multiple Info-Blocks

Alerts issued by EC through their trusted feed may contain multiple info blocks. Alerts with Multiple info blocks contain 2 different kinds of description, severity, certainty and urgency for the same Event type. In other words, these alerts contain 2 different set of values for the same Event type in 2 different info blocks, within the same alert.

Alerts with multiple info blocks vary slightly in the xml structure from alerts issued through the NAAD System interface.

Alerts issued from the NAAD system will not contain multiple info blocks.

## Rules for attachments

The following types of attachments are supported by the NAAD System:

### Attachment types:

- Audio file attachments, if included, must be in one of the MP3, WMA or Wav file formats.
- Image file attachments, if included, must be in either the png or jpeg file format.

### Attachment size:

- The cumulative size of all file attachments in any single Alert Message will not exceed 800 Kbytes prior to conversion to base64.

### Alert Message size:

- The size of any single Alert Message, including all file attachments must not exceed 5 Mbytes prior to conversion to base64.

### URL Attachments:

AGAs can also attach files using a link. To avoid potential issues, Pelmorex has recommended the following guidelines to AGAs:

1. Ensure the server where the URL is hosted is up and running at all times
2. The server where the URL is hosted can support reasonable traffic, and has sufficient bandwidth for users to grab the URL. If there is insufficient bandwidth for let's say 100 users at a time trying to connect to the server, it could result in LMDs getting disconnected from the server and not gaining access to the URL.



Please note that the NAAD System cannot guarantee the existence and validity of the attachment being referenced through a URL nor does the system store or provide these files. It is the Issuers sole responsibility to ensure the existence and validity of these attachments.

## Display of special characters for LMDs

Websites generally use the ISO standard which supports 1 million characters which is LESS than the UTF-8 standard the NAAD system uses. What this means for LMDs is that certain special characters used by AGA such as ☺, \$, # etc. may show up on their websites either differently or get replaced by "?" or by a blank space.

If normal keyboard characters (such as those on the keyboard) are used while creating an alert directly into the NAAD application most characters are supported. To avoid a potential issue, Pelmorex recommends that AGA avoid using special characters when creating an alert and do not cut and paste text from a Word document.

You can find more information on the ISO and UTF-8 standards below:

- Characters supported in ISO-8859-1 (also called Latin 1, which is the default encoding in Windows): [http://en.wikipedia.org/wiki/ISO/IEC\\_8859-1#Codepage\\_layout](http://en.wikipedia.org/wiki/ISO/IEC_8859-1#Codepage_layout)
- Characters supported in UTF-8: <http://www.utf8-chartable.de>

## Rules Governing NAAD System Testing & Test Messages

The purpose of these rules is to set out the policies and procedures for tests performed by Authorized Provincial/Territorial (P/T) Emergency Management Organizations (EMOs), Alerting Authorities and Pelmorex, to ensure Alert Messages are received and submitted successfully and that the NAAD System is available and operational at all times. To that end, the NAAD System supports two different ways of testing.

### **A. Test messages not intended for broadcast:**

1. Heartbeat Message
2. Test message with Message status: Test

### **B. Test messages intended for broadcast:**

1. Test message with Message status: Actual
2. Public awareness test messages.

To ensure “not intended for broadcast” and “intended for broadcast” Test Messages are easily identified and dealt with appropriately by LMDs, Authorized Government users must comply with the rules.

For further details, please refer to the [Test Message Policy V2.0](#) at this [LINK](#).



Please note that the Test Message Policy V2.0 is an updated version which is effective April 01<sup>st</sup>, 2015. It allows the possibility of selecting a test alert as Broadcast Immediate. Please discard any references/copies of the previous older Version 1.0 at your end.

## Sections to follow

The subsequent chapters of this document provide information on:

- How to listen to Satellite C band & Ku band and/or TCP feeds,
- Details on the GeoRSS auxiliary service,
- Description of the Heartbeat message,
- Sample Alert Messages,
- Information on Digital Signatures.

## Reference Documents

- CAP Standards
- CAP-CP Standards
- Statistics Canada Standard Geographical Codes

These and other documents can be found at:

<https://alerts.pelmorex.com/techinfo/currentcapmaterial/>

## User Resources

The NAAD System also provides a User Resource Centre. This is in the form of a website, where users (including LMDs) can view general NAAD System related information including a

list of vendors and distributors of equipment for LMDs. Users can also register on the website (for free) and receive further information and updates on the NAAD System.

For further information please visit:

<https://alerts.pelmorex.com/> [English]

<https://alerts.pelmorex.com/?lang=fr> [French]

Or contact our support team at:

[Support-PublicAlerting@Pelmorex.com](mailto:Support-PublicAlerting@Pelmorex.com)

## Chapter 2

# NAAD System Feed Specifications

This chapter includes...

- Satellite and TCP Streaming Feed – General Information
- Satellite Feed
- Summary and additional notes for the Satellite Feed
- Internet TCP Streaming Feed
- Summary and additional notes for the TCP Streaming Feed
- Internet GeoRSS Feed (based on Atom and GeoRSS Simple)
- Summary and additional notes for the GeoRSS Feed
- Troubleshooting Internet TCP Streaming Feed

## About NAAD System Feeds

The NAAD System provides 3 different communication channels in order to receive Alert Messages:

- **C Band Satellite**
- **Ku Band Satellite**
- **Internet TCP Streaming Feed**

A 4<sup>th</sup> auxiliary communication channel, **Internet GeoRSS Feed** (based on Atom and GeoRSS Simple) is also available but should not be used to feed a 24/7 automated system.

This chapter describes each of these different feeds.



'Satellite' and 'Internet TCP Streaming' Feeds are recommended for use by LMDs for real-time and or automated 24/7 applications. The 'Internet GeoRSS' Feed is an auxiliary feed for human access & for checking alerts, and should not be used for feeding a real time automated system.



An Alert Message received through any of the three main communications channels is identical byte by byte on the other communications channels.

## Satellite and TCP Streaming Feed – General Information

The start and end of each CAP-CP XML formatted Alert Message is detected using the start and end tags (<alert ... and </alert>). If the CAP-CP XML starts with the optional XML declaration (<?xml version=...), then the declaration is part of the CAP-CP XML and the encoding attribute should be used to process the data correctly.

## Alerts

Alert Messages in CAP-CP compliant format are sent to all feeds once they are received by the Pelmorex NAAD System. There will be slight differences in the actual time that the alerts are received by the LMD over these data feeds due to different bandwidth and connection speed constraints of the Satellite and Internet TCP feeds.

Alert Messages may occasionally be sent multiple times over a communications channel only if a transmission error was detected by the Pelmorex NAAD System and only on the communications channel where the transmission error was detected. This does not necessarily mean that the data received by the LMD was invalid/corrupted, but the LMD clients should always validate the data, and be capable of handling duplicate alerts.

For internet feeds, there are 2 geographical locations where the feed is available: Oakville and Montreal.

The CAP-CP XML form of the Alert Message will contain 1 or 2 XML signatures from which a LMD can verify that the alert is from a genuine source and/or from the NAAD System. Alerts will always have a NAAD System Digital Signature and may have an Issuer (AGA) Signature. When both are present, the NAAD System signature encompasses the AGA signature without invalidating the Issuer Signature.

Satellite and TCP Streaming feeds will contain the original Alert Message that was sent and any attachments will be in base 64. AGAs may include 'Links' to attachments in which case LMDs will need to retrieve the attachment from the location identified by the Issuer. To summarize, AGA may include attachments in two forms (including both simultaneously in the same message):

- Attachment(s) may be embedded in the message; embedded attachment(s) are in base64 and require extraction/base64 decoding to retrieve the original attachment
- Links to attachment(s) hosted on AGA/external systems in which case LMDs will need to retrieve it from the location identified by the AGA/link.

## NAAD Heartbeats

All NAAD System satellite and TCP streaming feeds include Pelmorex originated CAP-CP XML NAAD "Heartbeats". NAAD Heartbeat CAP-CP XML data is sent to allow LMDs to determine if the feed is operational. The Heartbeat also contains the list of the last (10) transmitted alerts on this feed. For the TCP Streaming Feed, heartbeats are sent at a specific interval (1 minute). For the Satellite Feed, heartbeats are sent at a specific interval, unless an alert is being sent at the same time. In this case, the alert has a higher priority and will be sent before the heartbeat.

NAAD heartbeats contain a history of the top 10 most recent alerts that were sent . See Appendix 1 for an example of the heartbeat and to see how the list of recent alerts is structured.

### 1. Satellite Feed

This feed is accessible from a satellite receiver on both C and Ku Band:

### C Band

For specific details about C Band feed reception, see Chapter 3, Section 1 Satellite Dissemination – C Band.

### Ku Band

For specific details about Ku Band feed reception, see Chapter 3, Section 2 Satellite Dissemination – Ku Band.

In order to receive the UDP packets from the satellite receiver (regardless of whether it is from C Band or Ku Band satellite), a UDP socket application (client) should be used by the LMD (NAAD System doesn't provide this application). This application will need to be in the same network segment as the satellite receiver, and it should register and receive packets sent to the IP multicast group: 224.0.10.10.

The UDP destination port 25555 must be used to receive data. The application should receive data from this port and reassemble the packets to receive CAP-CP XML data.

The UDP packets should be assembled in the sequence in which they are received, in order to reassemble the packets into CAP-CP XML data. There is no additional information used to indicate the sequence of the UDP packet's data within the CAP-CP XML.

In order to minimize the UDP packets re-ordering issue (since it could happen according to protocol specifications), LMD should connect the decoding system/computer directly to the satellite receiver using an Ethernet cable.

## Summary and additional notes for the Satellite Feed

- The data will come out of the satellite receiver as unidirectional IP from the RJ45 Ethernet connection.
- The data is sent using a IP multicast group address: 224.0.10.10
- The IP protocol used to multicast the data is UDP.
- The UDP destination port is 25555.
- Since UDP has limitation of about 64 KB in size, the Alert Messages are separated into segments.
- The size of a UDP segment is 1024 bytes (of usable data payload, this is not the actual Ethernet packet size)
- Alert Messages will always start at the beginning of a UDP packet, and all subsequent segments for the same alert are sent sequentially one after the other until the alert has been sent completely.
- Attachments will be embedded in the CAP-CP XML as Base64 encoded data in the resource tag.
- Heartbeats are sent at specific intervals (1 minute) to indicate that the system is up and running (see Appendix 1 for details on 'Heartbeats')

## 2. Internet TCP Streaming Feed

This feed is accessible through the Internet.

In order to receive this feed, a TCP/IP socket application (client) must be used by the LMD and it must be able to connect to the following domains:



- streaming1.naad-adna.pelmorex.com (Oakville)
- streaming2.naad-adna.pelmorex.com (Montreal)
- TCP port is 8080 (for both sites)

It is recommended for redundancy purposes to connect to both TCP streaming feeds, or to one of the satellite feeds (C band or Ku band) at the same time, and discard any duplicate alerts since under normal operation, both feeds will be active and sending alerts almost at the same time. If one feed is down, the application should try to reconnect at a pre-set interval while continuing to receive the data from the active feed.

In order to detect connection issues and missing alerts, the NAAD Heartbeat CAP-CP data is sent every minute. If the application does not receive any NAAD Heartbeats after an expected delay (2 minutes for example), then it is recommended that the application should start a reconnection procedure.

The NAAD Heartbeat CAP-CP data contains the list of recent alerts that were sent by the Pelmorex NAAD System on that specific feed. The application can use this list to detect if an alert has been missed. In this case, the LMD's application could retrieve it from the HTTP short term repository site (See 'Appendix 1 - Heartbeats' for details). Alert Messages are kept for 48 hours in the HTTP short term repository for retrieval purposes by automated systems.

See Appendix 1 for an example of the heartbeat and to see how the list of recent alerts is structured.

As soon as the application has connected, alerts can be received; there is nothing that should be sent by the application itself to initiate the reception. It should just wait to receive alerts and heartbeats from the connected TCP socket.

Since this feed is a live TCP stream of alerts, the start and end tags of the CAP-CP XML document (<alert ... and </alert>) must be used to detect the start and end of an Alert Message within the stream. There are no special or proprietary headers added to the data, only raw XML is transmitted.

## Summary and additional notes for the TCP Streaming Feed

- Alert Messages are provided as a data stream using TCP/IP protocol.
- The host and port of the socket to connect to receive this stream is:
  - streaming1.naad-adna.pelmorex.com (Oakville)
  - streaming2.naad-adna.pelmorex.com (Montreal)
  - TCP port: 8080
- The start and end of an alert is detected using the start and end tags of the XML document (<alert ... and </alert>). There are no special or proprietary headers added to the data, only raw XML.
- If the alert contains an XML declaration (<?xml version=...) then the encoding attribute should be used to process the data correctly.
- Heartbeats are sent a specific interval (1 minute) to indicate the connection is alive (see Appendix 1)

### 3. Internet GeoRSS Feed

The Pelmorex NAAD System GeoRSS feed is provided as an alternate method for viewing alerts but is not intended for feeding 24/7 automated systems.

This feed is accessible through the Internet and is formatted in Atom Syndication Format (See: [http://en.wikipedia.org/wiki/Atom\\_%28standard%29](http://en.wikipedia.org/wiki/Atom_%28standard%29)) and also includes the GeoRSS Simple support (see: <http://www.georss.org/simple>) to include additional geographical information related to the affected area included in the original alert. This feed can be viewed using any RSS reader that supports an Atom feed; however standard RSS readers (such as Internet Explorer, Firefox, etc.) will only display the RSS/Atom portion, and not the geographical information included by the GeoRSS portions.

In order to see the geographical information, a GeoRSS reader must be used. The GeoRSS feed contains the last 48 hours of alerts listed as Atom <entry> elements. Each alert info element will be represented as an entry in the feed. Categories in the feed can be used to filter the entries. For example, *language=en-CA* category will allow the RSS Reader to display only entries for the en-CA language/locale.

Pelmorex official URLs to access the GeoRSS feed are:

- <http://rss1.naad-adna.pelmorex.com> (Oakville)
- <http://rss2.naad-adna.pelmorex.com> (Montreal \*)



\* It is the responsibility of the LMD to reconnect to the second site if the first site is down, and vice-versa. Under normal conditions, both sites should be active.

The GeoRSS feed provides list of alerts with some basic information; reference is made to the real alert which is in the same CAP-CP format and identical to the version received via satellite or TCP streams.



The GeoRSS only contains the geometry information and not the geo-codes as they are in CAP-CP, so it can't replace completely the geography defined in the real alert.



The GeoRSS is only a subset of the actual Alert Message and should not be used as a base for public display by LMDs.

### Summary and additional notes for the GeoRSS Feed

- The alerts from the last 48 hours are formatted into a RSS feed in a simple GeoRSS Atom format
- The URLs for this feed are:
  - <http://rss1.naad-adna.pelmorex.com> (Oakville)
  - <http://rss2.naad-adna.pelmorex.com> (Montreal)
- Each Alert Message is presented as an entry in the feed
- For each entry:

- A URL to the Alert Message XML file is present
- URLs to attachment files are present, if they exist in the Alert Message.
- **Note:** most (Geo) RSS Readers can only display 0 or 1 attachment(s)
- Filter category tags are present to allow the (Geo) RSS Reader to filter entries in the feed. Example: Internet Explorer is a reader that can filter entries using the category field.

#### 4. Troubleshooting Internet TCP Streaming Feed

Internet connections from Last Mile Distributors (LMD) must meet the minimum specifications outlined below. Connections that do not meet the standards will hinder alerts from being distributed and may be dropped by Pelmorex at its own discretion.

|  |   |  |
|--|---|--|
| Web Interface Connection Recommendations | <ul style="list-style-type: none"> <li>• Most recent up to date Java</li> <li>• Most recent version of a Web browser</li> </ul>   |  |
| Feeds Connection Recommendations         | <p>Average users home internet speed:</p> <ul style="list-style-type: none"> <li>• Standard 1.5 Mbps downstream speed</li> <li>• 384 kbps upstream speed</li> </ul> <p>Socket feed connection timeout times:</p> <ul style="list-style-type: none"> <li>• 2 ms when connection is established</li> <li>• 1,005 ms when host is alive but not listened to on the specified socket port</li> <li>• 21,000 ms when host is down</li> </ul> | <ul style="list-style-type: none"> <li>• Dial-up internet connection is not recommended</li> <li>• A normal DSL internet with 6mb download (minimum)</li> <li>• The ability to reconnect within 1 minute if disconnected</li> <li>• Missed alerts can be retrieved using heartbeats</li> </ul> |

If internet connections are dropped by either the LMD or Pelmorex, the last 10 alerts are available through the NAAD heartbeat CAP-CP data. This list is used to detect any missed alert. LMD's application could retrieve it from the HTTP short term repository. Alert Messages are kept for 48 hours in the HTTP short term repository for retrieval purposes by automated systems. Alerts can be received as soon as the application has connected (it waits to receive alerts and heartbeats from the connected TCP socket).

Alerts are also archived at [alerts.pelmorex.com](https://alerts.pelmorex.com/filearchiveaccess/) (See: <https://alerts.pelmorex.com/filearchiveaccess/>).

## Chapter 3

# Satellite Dissemination

This chapter includes...

- Satellite Dissemination – C Band
- Satellite Dissemination – Ku Band
- Addendum A – C Band
- Example A: Configuring CISCO D-9850 Receiver (Primary Feed)
- Example B: Configuring CISCO D-9850 Receiver (Secondary Feed)
- Addendum B – Ku Band

## About Satellite Dissemination

The NAAD System provides satellite dissemination through C Band and Ku Band as described below.



While receiving alerts through Satellite, LMDs should connect directly to the receivers through the Ethernet port (without any switch, router etc. in the middle). Failing to do so will not guarantee the packet order and they might receive some packets in the wrong order.

### 1. Satellite Dissemination – C Band

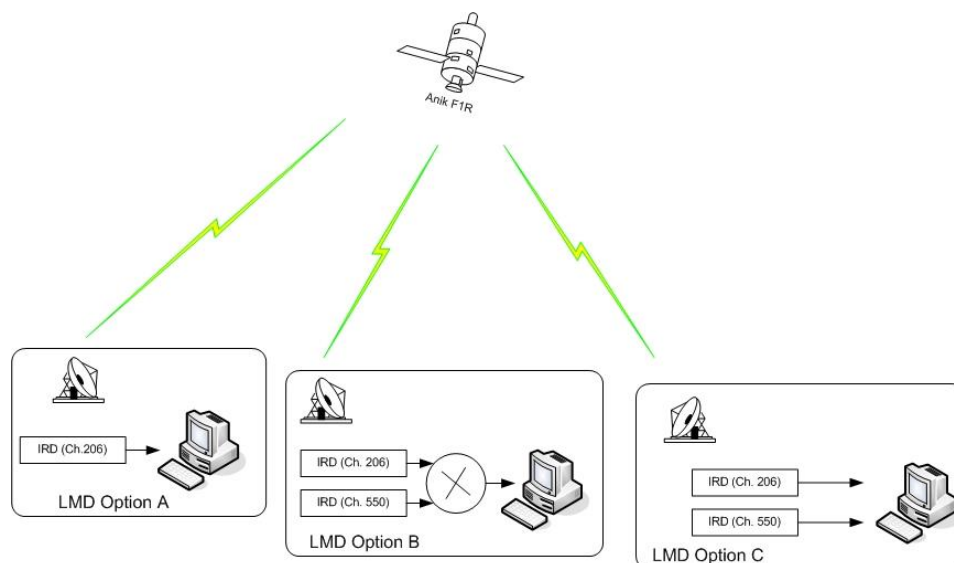
C-Band dissemination is provided by Telesat over Anik F1R Satellite. It is expected that most BDUs and TV broadcasters already possess a receiving satellite antenna pointed to this satellite.

The main C Band feed is on virtual channel 206. In the unlikely event that the main feed will be disabled then the service will be transferred to the virtual channel 550.

There are three ways a receiving site may be equipped to receive alerts messages over the C-Band. Please note, Pelmorex is also disseminating alerts through the internet and KU band satellite.

1. A simple, approach, option A, is to have one dish and one receiver (IRD). (The downside of this approach is that requires manual change between virtual channels if alerts feed fails for any reason.
2. If the LMD wants to have a transparent operation when the feeds are being switched then the receiving site should be equipped with two receivers (IRD) and data routers (option B)

3. Instead of using the data router, software application may accept two data feeds from two receivers (option C).



**Figure 1 – Satellite Dissemination – C Band**

Each receiver (IRD) must be tuned to assigned virtual channel. Please see addendum A for the technical specifications.

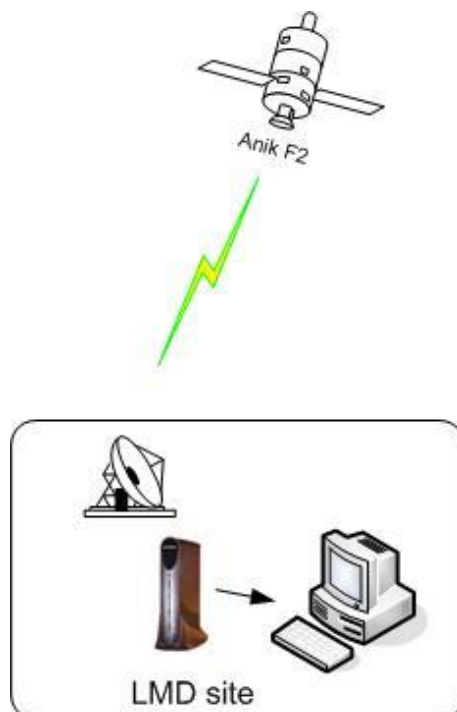


For redundancy, TCP or Ku feeds may also be used as an alternative instead of monitoring the 2 C Band channels.

## 2. Satellite Dissemination – Ku Band

Due to rain and snow fades, the Ku Band dissemination system has been designed with two simultaneous up/down links at all times (active - active up/down link). The receiving terminal is configured to receive either primary or secondary feed or both feeds simultaneously.

The NAAD System Ku Band dissemination is provided by iMpACT satellite telecommunication service. In order to receive the NAADS KU band signal, the LMD must purchase a HN7700S iMpACT terminal from TELESAT. TELESAT will define and commission the terminal and will ship the unit to the LMD. Beside the iMpACT terminal, the LMD site must be equipped with a satellite antenna (dish) pointed to the Anik F2 satellite. Telesat can provide installation services for LMDs if required. Pelmorex does not provide or pay for equipment or installation services. For more technical details please see Addendum B.



**Figure 2 – Satellite Dissemination – Ku Band**

## ADDENDUM A – C Band

- A minimum 3 meter C-Band dish pointed to Anik F1R is required at the receiving site.
- Any DVB-S or DVB-S2 receiver with IP output is compatible with the service. PELMOREX is using a Cisco D 9850 receiver (IRD) with IP output.
- Primary feed: transponder 9B (4,060 MHz), vertical polarization, virtual channel 206.
- Secondary feed: transponder 10B (4,100 MHz), vertical polarization, virtual channel 550.
- Primary feed: Network ID: 2
- Secondary feed: Network ID: 1
- Main frequency: 1050.00 MHz
- FCC Rate: 7/8
- Symbol Rate: 28.3465
- Bit rate: 500 Kbits/sec (500000) (could be increased in the future if needed)

## EXAMPLE A: CONFIGURING CISCO D-9850 RECEIVER (PRIMARY FEED)



Connect the LNB to the RF # 1  
Connect the AC cord



Configuration



Press MENU



Press the arrow right button to select PRESET  
Press SELECT button

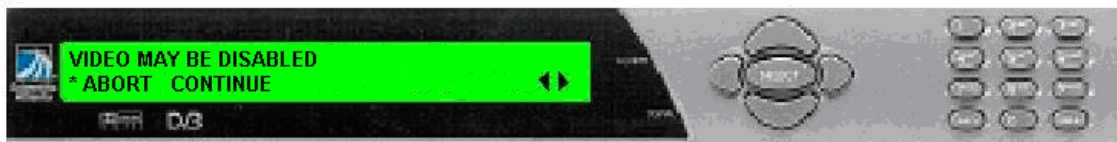


Press the arrow button down



Press SELECT





Press CONTINUE



Press SELECT and dial the default frequency 04.0600  
Press SELECT



Press the arrow button down to go to the second menu



Press the arrow right to change the NET ID  
Press SELECT  
Dial the value 00002  
Press SELECT



Press MENU



Press the arrow right button to select CONTINUE  
Press SELECT





Press MENU  
Dial the virtual channel 206  
Press SELECT



The signal led should be now on.

## EXAMPLE B: CONFIGURING CISCO D-9850 RECEIVER (SECONDARY FEED)



Connect the LNB to the RF # 1  
Connect the AC cord



PRESS MENU



SELECT PRESET



USE THE ARROW RIGHT TO SELECT PRESET

PRESS SELECT



PRESS THE ARROW DOWN



PRESS SELECT



USE THE ARROW RIGHT AND SELECT CONTINUE  
PRESS SELECT



USE THE PAD KEYS AND ENTER 04.100  
PRESS SELECT



PRESS MENU



USE THE ARROW RIGHT TO SELECT CONTINUE  
PRESS SELECT



PRESS MENU  
DIAL 550 SELECT



SIGNAL LIGHT SHOULD BE ON

## ADDENDUM B – Ku Band

- Ku-Band antenna 0.98m to 2.4m on Anik F2  
The size of the antenna depends on the geographical position of the receiving site.  
Please consult Telesat for detailed information.
- HN7700S iMpACT terminal (must be purchased from Telesat)
- Configuration to be done by Telesat
- Bit rate: 500 Kbits/sec (500000) (could be increased in the future if needed)

## Appendix 1: Heartbeats

### Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>5A89A6FD-0D89-1C6C-46D5-B535F61C068F</identifier>
  <sender>NAADS-Heartbeat@NAADS@PelmorexCommunicationsInc.</sender>
  <sent>2011-06-22T05:06:49+00:00</sent>
  <status>System</status>
  <msgType>Update</msgType>
  <scope>Public</scope>
  <code>profile:CAP-CP:0.3</code>
  <references>NAADS-Heartbeat@NAADS@PelmorexCommunicationsInc.,DD9216B4-
2A6C-8514-4332-85B7359FE2E0,2011-06-22T04:59:00+00:00</references>
</alert>
```

The format of the heartbeats conforms to the same CAP Oasis 1.2 and CAP-CP standards as Alert Message disseminated by the NAAD System do.

Heartbeats are sent each minute on both Internet TCP Streaming and Satellite feeds. The GeoRSS feed does not contain NAAD heartbeats.

- Each entry in the <references> list is composed of the 3 elements (Sender, Identifier, Sent) with a comma (,) between Sender-Identifier and Identifier-Sent) and a space between each entry.
- Entries are listed from the oldest to the most recent transmission based on the transmission time (not the issued time); most of the time, thus will correspond also to the sequence they have been issued too.
- References is used here to express a list and does not means any links/references between the alerts identified in the list; similarly, the list does not imply any update/cancel on the identified alerts. This is purely a list of recent transmission on the feed from which the Heartbeat is received.



Lists may differ slightly between communication channels (Feeds) as heartbeats are not synchronized between channels. Sent and ID are the same for the same alerts whatever channels as those are the Issue/ID from the Issuer.



Heartbeats are not digitally signed and respect CAP-CP formatting.



The heartbeats can be identified easily by checking the status is System and Sender is NAADS-Heartbeat.

## Retrieving missed alerts using heartbeat information:

In order to retrieve alerts that were missed and that are referenced in the heartbeats, a HTTP URL can be recreated using the following method:

`http://[capcp-site-domain]/[SENT_DATE]/[SENT]I[IDENTIFIER].xml`

Where:

- [capcp-site-domain] = [capcp1.naad-adna.pelmorex.com](http://capcp1.naad-adna.pelmorex.com) (Primary Site -> Oakville) or [capcp2.naad-adna.pelmorex.com](http://capcp2.naad-adna.pelmorex.com) (secondary Site -> Montreal)
- [SENT\_DATE] = The date portion (YYYY-MM-DD) of the sent date/time from the <references> element found in the heartbeat.
- [SENT] = The sent date/time from the <references> element found in the heartbeat. Including time and time zone information.
- [IDENTIFIER] = The identifier found inside the <references> element in the heartbeat.

### Additional important notes:

- Some characters are substituted for other ones, this **substitution must be applied** to create the final valid URL:
  - The minus sign (- or dash) is replaced by underscore character (\_)
  - The plus sign (+) is replaced by P
  - The colon character (:) is replaced by underscore character (\_)
  - This replacement must be done only on the [SENT] and [IDENTIFIER] part of the URL.

### Examples:

Information from the heartbeat:

<references>**NAADS-Heartbeat@NAADS@PelmorexCommunicationsInc.,DD9216B4-2A6C-8514-4332-85B7359FE2E0,2011-06-22T04:59:00+00:00**</references>

### Resulting URL:

`http://capcp1.naad-adna.pelmorex.com/2011-06-22/2011_06_22T05_06_49p00_00I5A89A6FD_0D89_1C6C_46D5_B535F61C068F.xml`

and (any of the 2 URLs will work)

`http://capcp2.naad-adna.pelmorex.com/2011-06-22/2011_06_22T05_06_49p00_00I5A89A6FD_0D89_1C6C_46D5_B535F61C068F.xml`



Please note that alerts are temporarily kept at this URL. Typically for up to 4/5 days. Any older alerts if referenced through this link will not be available.



## Appendix 2: Sample Alert Messages

Samples of Alert Messages as if they were received from C band, Ku band or TCP stream or retrieved from missed alerts retrieval site are described below:

### Pelmorex NAAD System Alert Message Examples in CAP-CP format

The following Pelmorex NAAD System Alert Message examples are based on CAP-CP beta version 0.3A and presented in valid XML format as defined by the CAP Oasis 1.2 XML schema. Encoding is UTF-8.

#### **Example #1 Alert Message No Attachment**

This example contains an Alert Message with NAAD System Signature and without an attachment.

[Click here](#) to download Example # 1.

#### **Example #2 Alert Message with Embedded Large Audio File**

This example contains an Alert Message with NAAD System Signature and an embedded attachment (in base64) of an audio file in MP3 format.

[Click here](#) to download Example # 2.

#### **Example #3 Alert Message with Multiple Embedded Audio Files**

This example contains an Alert Message with NAAD System Signature with 2 embedded attachments (in base64) of 2 audio files in MP3 format.

[Click here](#) to download Example # 3.

#### **Example #4 Alert Message with a URL Link to a Large Audio File**

This example contains an Alert Message with NAAD System Signature and a URL inserted by Issuer, specifying the location of an attachment of an audio file in MP3 format. *[Note: This example is the same as example #2 except the attachment is linked instead of being embedded]*

[Click here](#) to download Example # 4.

#### **Example #5 Alert Message with URL Links to Multiple Audio Files**

This example contains an Alert Message with NAAD System Signature and a URL inserted by Issuer, specifying the locations of attachments of 2 audio files in MP3 format. *[Note: This example is the same as example #3 except the two attachments are linked instead of being embedded.]*

[Click here](#) to download Example # 5.

#### **Example #6 Alert Message with Free hand drawn polygon**

This example contains an Alert Message with NAAD System Signature and a free hand polygon specifying a more specific location of an event

[Click here](#) to download Example # 6.

**Example #7 Alert Message with Free hand drawn circle**

This example contains an Alert Message with NAAD System Signature and a free hand circle specifying a more specific location of an event

[Click here](#) to download Example # 7.

**Example #8 Alert Message with Free drawn point**

This example contains an Alert Message with NAAD System Signature and a free hand point specifying a more specific location of an event

[Click here](#) to download Example # 8.

**Example #9 Alert Message with "Minor Update"**

This example contains an Alert Message with NAAD System Signature and the "minor update feature" selected

[Click here](#) to download Example # 9.

**Alert Locations/Area:**

In the latest release 7.0, NAAD System now provides issuers the opportunity to draw or import a polygon, circle or a point that represents the alert's effected area. These are called Freehand Drawn Shapes. This results in 2 kinds of alerts: alerts without any freehand drawn shapes and alerts containing one or more free hand drawn shapes. Both have a slight difference, explained below. Please refer to first part of Appendix 2 to see sample alerts with or without freehand drawn shapes.

**Alerts without freehand drawn shapes:**

These alerts will contain one or more SGC locations in the alert's Area block. For Alerts containing multiple locations, the SGC regions (polygons) in the alert's Area section appear in order of selection, as selected from the NAADS User Access System interface. Each SGC will be added as a separate polygon and will include the geocode as well in the same Area block.



NAADS interface does not recommend or check the sequence preference for location selections. This selection order preference is solely the Issuer's own choice. For instance an Issuer can select a sub-division first and then select the corresponding province. This order is not changed and will appear as is, in the Alert Message.

The sequence of Polygons and their corresponding Geocodes is the same as selected by an Issuer. The first Polygon has the first Geocode, second Polygon has the second Geocode and so on. See example below:

```
<area>
  <areaDesc>Test Area</areaDesc>
```



```

<polygon>49.828018,-101.41931 49.000079,-101.36248 49.000076,-
95.153115 94.837808 60,-94.822871 60,-101.999999 55.8128,-101.999999
49.828018,-101.41931</polygon>
<polygon>49.000038,-96.784563 49.000076,-95.153115 50.395818,-
95.152917 50.327214,-96.353685 49.266301,-96.376094 49.266276,-
96.780004 49.000038,-96.784563</polygon>
<polygon>49.000038,-96.784563 49.266276,-96.780004 49.266301,-
96.376094 49.186899,-97.310227 49.095757,-97.214918 49.022915,-
97.201883 49.000038,-96.784563</polygon>
<geocode>
  <valueName>profile:CAP-CP:Location:0.3</valueName>
  <value>46</value>
</geocode>
<geocode>
  <valueName>profile:CAP-CP:Location:0.3</valueName>
  <value>4601</value>
</geocode>
<geocode>
  <valueName>profile:CAP-CP:Location:0.3</valueName>
  <value>4602</value>
</geocode>
</area>

```



### Alerts with freehand drawn shapes:

Use of freehand drawn shapes is optional and if an issuer adds them to an alert these can be easily identified. An issuer can add a freehand drawn Polygon or Circle (only one of these at a time) with or without a Point.

### Freehand Polygon:

Free hand drawn polygon is added to the alert in 2 places. One as a parameter in the Info block:

```

- <parameter>
  <valueName>NAADS:InternalUse:1</valueName>
  <value>Polygon</value>
</parameter>

```

And also as a Polygon in the Area section:

```

- <area>
  <areaDesc>Capital H and Capital</areaDesc>
  <polygon>48.346288,-123.669953 48.355871,-123.664117
48.354502,-123.652272 48.336818,-123.652787 48.339214,-
123.673901 48.346288,-123.669953</polygon>
- <geocode>
  <valueName>profile:CAP-CP:Location:0.3</valueName>
  <value>5917054</value>
</geocode>
- <geocode>
  <valueName>profile:CAP-CP:Location:0.3</valueName>
  <value>5917054</value>
</geocode>

```

Please note that all other SGC location polygons will not be included in the alert. Only this freehand shape will be included as Polygon in the area block. However, the geocodes for all SGC locations will be included in the Area block. If we remove the freehand polygon, then Polygons for each individual SGC location will be included.

### **Freehand Circle:**

Free hand drawn circle is added to the alert in 2 places. One as a parameter in the Info block:

```
- <parameter>
  <valueName>NAADS:InternalUse:1</valueName>
  <value>Circle</value>
</parameter>
```

And also as a Circle in the Area section:

```
- <area>
  <areaDesc>Capital H and Capital</areaDesc>
  <circle>48.345910,-123.661900 5</circle>
- <geocode>
  <valueName>profile:CAP-CP:Location:0.3</valueName>
  <value>5917054</value>
</geocode>
- <geocode>
  <valueName>profile:CAP-CP:Location:0.3</valueName>
  <value>5917054</value>
</geocode>
- <geocode>
```

Please note that all other SGC location polygons will not be included in the alert. Only this freehand circle will be included in the area block. However, the geocodes for all SGC locations will be included in the Area block. If we remove the freehand circle, then Polygons for each individual SGC location will be included.

### **Freehand Point (Event Location):**

Point is also called Event Location and it can be added as a parameter in the Info block of an alert:

```
- <parameter>
  <valueName>layer:NAADS:1.0:eventLocation:point</valueName>
  <value>49.009327,-122.815854</value>
</parameter>
```

**NEW**

### **Minor Update:**

This is an optional feature, only available when alert 'Msg. Type' is selected as 'Update'. It identifies the change to an alert as minor consistent with CAP-CP 4.0. It is included separately for each language block. If an alert has a minor update selected, it will include a value and also might have (optional) comment. The comment is added in the <note> of the alert. The value will be one of the following:

|                   |   |
|-------------------|---|
| <b>Text</b>       | When a change has occurred between <info> blocks where some free form text content may have been added or modified, the value of "text" should be used in the <info> block(s) where applicable                            |
| <b>Correction</b> | When a correction is made to some of the free form content, perhaps because of an error, spelling mistake or omission, the value of "correction" should be used in the <info> block(s) where applicable                   |
| <b>Resource</b>   | When the addition, modification, or removal of a <resource> block and its associated content takes place relative to the previous message, the value of "resource" should be used in the <info> block(s) where applicable |
| <b>Layer</b>      | When the addition, modification, or removal of layer based values takes place relative to the previous message, the value of "layer" should be used in the <info> block(s) where applicable                               |
| <b>Other</b>      | When the content change doesn't meet the criteria of the other parameter values, the value of "other" should be used in the <info> block(s) where applicable  |
| <b>None</b>       | When no change has occurred in an <info> block relative to the previous message, the value of "none" should be used   |

### Sample Minor Update in alert XML:

Minor update is added as follows:

```
- <parameter>
  <valueName>profile:CAP-CP:0.4:MinorChange</valueName>
  <value>other</value>
</parameter>
```

Comment is added to <note>:

```
<note>Minor Update: en-CA|Sample test content</note>
```

For minor update if <Note> is present, it will always have a prefix "Minor Update:" at the beginning. If an alert has multiple languages and if there are multiple comments for minor update, then the <note> will have all comments combined in one string separated by ^ and preceded by the language identifier, example:

```
<note>Minor Update: en-CA|Test EN Comment^fr-CA|Test FR Comment</note>
```

If the issuer doesn't provide any comment for minor update, the alert will not have a <note> for it.

## Appendix 3: Broadcast Intrusive Alerts

The concept of Broadcast Intrusive (Immediate) alerts is supported in NAADS. The Broadcast Intrusive criterion is based on the SOREM's list of CAP-CP event codes and their respective CAP severity, urgency and certainty values (list attached as follows). If the Broadcast Intrusive criterion is met, the sender will be notified on the interface while still creating the alert. Once the alert is sent, a Broadcast Intrusive flag value will be set as Yes or NO, respectively, in the alert. From this release forward every NAADS alert will now contain this parameter in the alert's XML form. Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>B024E3AB-D421-813C-BE9C-FD6591FE8082</identifier>
  <sender>SDA@PublicAlerting@PelmorexCommunicationInc.</sender>
  <sent>2011-10-13T18:45:09-04:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <code>profile:CAP-CP:0.3</code>
  <info>
    <language>en-CA</language>
    <category>Safety</category>
    <category>Infra</category>
    <event>Dam Overflow</event>
    <urgency>Immediate</urgency>
    <severity>Extreme</severity>
    <certainty>Observed</certainty>
  </info>
  <eventCode>
    <valueName>profile:CAP-CP:Event:0.3</valueName>
    <value>damOverflow</value>
  </eventCode>
  <expires>2011-10-14T09:43:00-04:00</expires>
  <senderName>Pelmorex</senderName>
  <headline>damOverflow</headline>
  <description>damOverflow</description>
  <instruction>en-CA</instruction>
  <parameter>
    <valueName>layer:SOREM:1.0:Broadcast_Immediately</valueName>
    <value>Yes</value>
  </parameter>
  <area>
    <areaDesc>Test Area</areaDesc>
    <polygon>48.250074,-88.836514 48.304678
      :
      :
      :
```

When the alert meets the "Broadcast Immediately" criteria, following will be the flag value:

```
<parameter>
  <valueName>layer:SOREM:1.0:Broadcast_Immediately</valueName>
  <value>Yes</value>
</parameter>
```

In all other cases:

```
<parameter>  
<valueName>layer:SOREM:1.0:Broadcast_Immediately</valueName>  
<value>No</value>  
</parameter>
```

## Broadcast Intrusive SOREM List

| <b>Tier I</b>       | <b>Event Code</b> | <b>CAP Code for Urgency</b> | <b>CAP Code for Severity</b> | <b>CAP Code for Certainty<sup>iii</sup></b> | <b><u>Additional Comments</u></b>   |
|---------------------|-------------------|-----------------------------|------------------------------|---|---|
| Air Quality         | airQuality        | Immediate                   | Severe or Extreme            | Observed                                    |   |
| Civil               | civilEmerg        | Immediate                   | Severe or Extreme            | Observed                                    | Definition is required but intention is to cover events such as large riots |
| Criminal Activity   | terrorism         | Immediate                   | Severe or Extreme            | Observed                                    |   |
| Dangerous Animal    | animalDang        | Immediate                   | Severe or Extreme            | Observed                                    |   |
| Fire                | wildFire**        | Immediate                   | Severe or Extreme            | Likely or Observed                          | Definition required and maybe customized depending on regional significance |
| Fire                | industryFire      | Immediate                   | Severe or Extreme            | Observed                                    |   |
| Fire                | urbanFire         | Immediate                   | Severe or Extreme            | Observed                                    | Definition required and maybe customized depending on regional significance |
| Fire                | forestFire**      | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Flood               | stormSurge**      | Immediate                   | Severe or Extreme            | Observed                                    |   |
| Flood               | flashFlood        | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Flood               | damOverflow       | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Geophysical         | earthquake        | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Geophysical         | magnetStorm       | Immediate                   | Severe or Extreme            | Likely or Observed                          | Not a thunderstorm. Can be solar flare                                      |
| Geophysical         | landslide         | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Geophysical         | meteor            | Immediate                   | Severe or Extreme            | Observed                                    |   |
| Geophysical         | tsunami**         | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Geophysical         | lahar             | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Geophysical         | pyroclasticS      | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Geophysical         | pyroclasticF      | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Geophysical         | volcanicAsh       | Immediate                   | Severe or Extreme            | Likely or Observed                          |   |
| Hazardous Materials | chemical          | Immediate                   | Severe or Extreme            | Observed                                    |   |

| Tier I              | Event Code   | CAP Code for Urgency | CAP Code for Severity | CAP Code for Certainty <sup>iii</sup> | Additional Comments                    |
|---------------------|--------------|----------------------|-----------------------|---------------------------------------|--|
| Hazardous Materials | biological   | Immediate            | Severe or Extreme     | Observed                              |  |
| Hazardous Materials | radiological | Immediate            | Severe or Extreme     | Observed                              |  |
| Hazardous Materials | explosives   | Immediate            | Severe or Extreme     | Likely or Observed                    |  |
| Hazardous Materials | fallObject   | Immediate            | Severe or Extreme     | Observed                              |  |
| Health              | drinkingWate | Immediate            | Severe or Extreme     | Observed                              | Impact to supply                       |
| Missing Person      | amber        | Immediate            | Severe or Extreme     | Observed                              |  |
| Utility             | 911Service   | Immediate            | Severe or Extreme     | Observed                              | Shutdown of service and call to action |
| Storm               | hurricane    | Immediate            | Severe or Extreme     | Observed                              |  |
| Storm               | thunderstorm | Immediate            | Severe or Extreme     | Observed                              |  |
| Storm               | tornado      | Immediate            | Severe or Extreme     | Likely or Observed                    |  |

\*"Emergency Public Alert" is defined in the NAAD Authorized User Agreements as an "Alert Message issued by an Authorized Government Agency or an Authorized User in respect of an imminent or unexpected threat to life caused by severe weather disturbances, natural disasters or other emergencies that meets the criteria for immediate distribution in the Standards."

<sup>i</sup> COMMON ALERTING PROTOCOL VALUES FOR 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
- "Unknown" - Urgency not known

<sup>ii</sup> COMMON ALERTING PROTOCOL VALUES FOR SEVERITY

- "Extreme" - Extraordinary threat to life
- "Severe" - Significant threat to life
- "Moderate" - Possible threat to life
- "Minor" - Minimal to no known threat to life
- "Unknown" - Severity unknown

<sup>iii</sup> COMMON ALERTING PROTOCOL VALUES FOR CERTAINTY

- "Observed" - Determined to have occurred or to be ongoing
- "Likely" - Likely ( $p > \sim 50\%$ )
- "Possible" - Possible but not likely ( $p \leq \sim 50\%$ )
- "Unlikely" - Not expected to occur ( $p \sim 0$ )
- "Unknown" - Certainty unknown

## Appendix 4: Digital Signatures

For security reasons and being in-line with CAP – V1.2, Alert Messages will contain 1 or 2 signatures.

1. First one is a digital signature produced by the Issuer (AGA) allowing verification to Alerts as being genuine to that specific Issuer and not tempered with. This signature is optional and is at the discretion of the Issuer's organization. So it may or may not be present.
2. Second is the NAAD System's digital signature in the alert message in addition to the Issuer's signature. It will always be present in alerts disseminated by NAAD System, but not in Heartbeat messages. It may be used by LMD's to confirm that the Alert Messages are received from the NAAD System.

### LMD point of view:

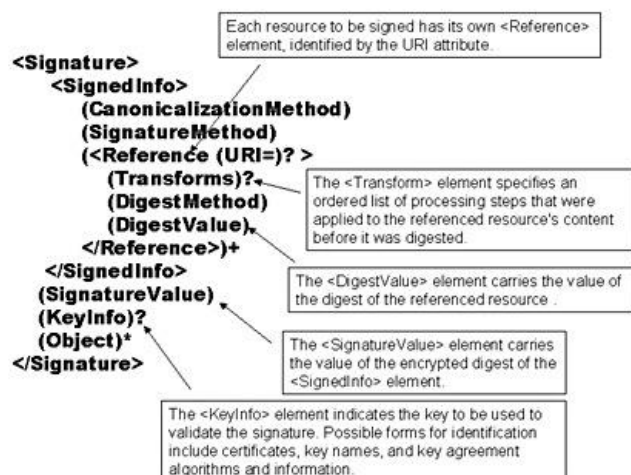
Alert Messages are not encrypted and are human readable regardless whether signatures are present. It is up to the discretion of the LMD to verify or ignore alert signatures.

When an Alert is received, the Last Mile Distributor has the option of checking either or both of the signatures to validate that the Alert did originate from NAADS system (i.e. not tampered in internet transmission after issuing) and also validate that the original Alert Message from the issuer is genuine and intact.

It is recommended that LMDs verify signatures for all Alert Messages intended to be displayed to the Public. When both signatures are present, it is preferable to check Issuer signature as it verifies the originators source.

### Verification Process:

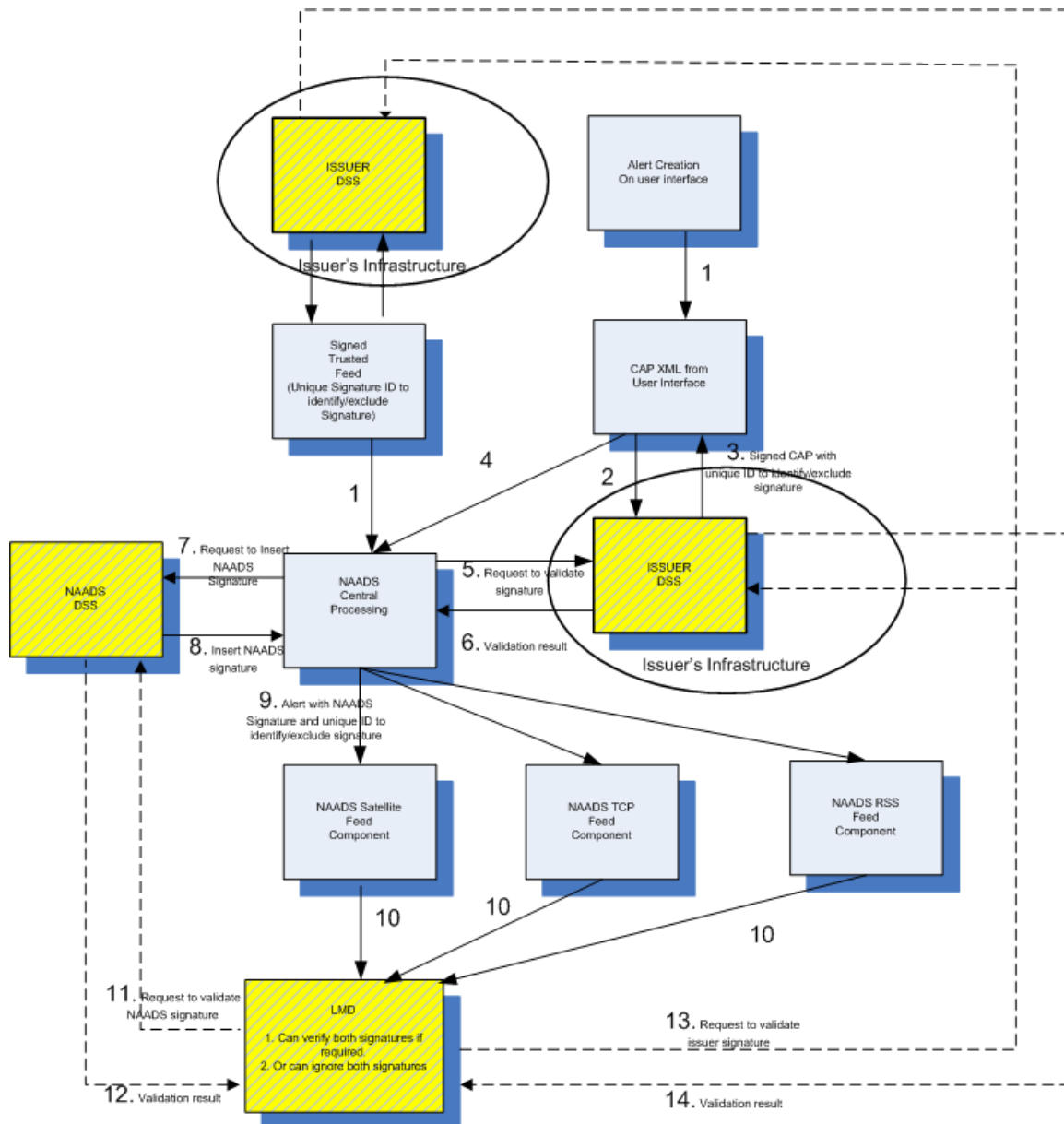
Digital signatures are included in the CAP 1.2 specification and utilize the XML-Sig standard. The XML-Sig standard identifies the various elements of the signature as below:



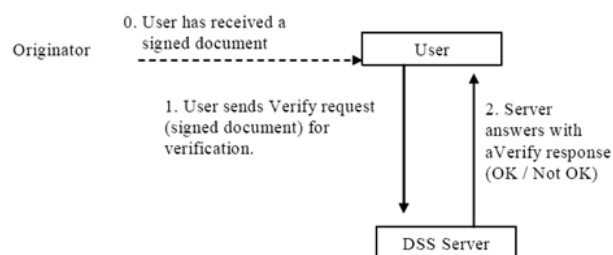
The data flow for the overall solution is as follows (Refer to Figure on next page). To make it easier for the LMDs, points that are of concern for an LMD are shown in **BOLD** text:



1. Issuer creates Alert Message through the NAADS user interface (1 in drawing)
2. Issuer submits Alert Message for signing through the NAADS user interface to the DSS of their organization. The Message is signed and the issuer then submits it to NAADS central processing through the NAADS user interface (2 & 3). This step is optional depending on whether issuer adds their signature.
3. NAADS central processing receives the Message. (4)
4. NAADS validates the signature by verifying against the issuer DSS (5 & 6). This guarantees no tampering in transmission. If the signature is not validated the Alert Message will be rejected and the issuer notified. This step is optional depending on whether issuer adds their signature.
5. **NAADS central processing adds its own signature using NAADS DSS (7 & 8)**
6. Alert Message which has two signatures is delivered by various mechanisms to LMD (9&10). If issuer has no signing DSS, only NAADS signature will be appended to the Message.
7. **LMD verifies the Message is sent by NAADS by validating NAADS digital signature against NAADS DSS. (11&12) This verifies that Message is not tampered in transmission from NAADS to LMD.** If this is valid, then LMD can further validate that original Alert is not modified or tampered in any way from the original issuing source by validating the issuer's signature against the issuing organization DSS. (13 &14). For both these validations, the LMDs will need to form XML based SOAP requests on https (following the OASIS-DSS standard) to the NAADS/Issuer DSS to get the signatures validated.
8. Once both validations are successful, the LMD can process the actual Alert Message. **If the Message was signed only by NAADS, LMD will validate against NAADS DSS only.**
9. **LMD's that prefer not to process either signature can just ignore the signatures and process the alert. LMD's that prefer to valid just one signature can filter out either signatures using XPath or other mechanisms and validate the required signature.**
10. **LMD's can verify the NAADS Signature by making a SOAP request on https (following the OASIS DSS protocol) to either DSS servers (as NAADS has a redundant infrastructure) indicated in the NAADS Digital signature as part of SignatureProperty ID element.** They can also verify locally (without making a request to DSS) if they have their own cryptographic verification tools using the information in KeyInfo part of the digital signature.



## Validating a Signed Message:



## Sample Messages – Digital Signature:

This section shows sample CAP-CP Alert Messages.

- Alert Message with no digital signature
- Alert Message with digital signature
- DSS Verification Request
- DSS Verification Response
- DSS Verification Response Failed

### 1. Alert Message with no digital signature

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>A2433D85-DB53-263A-998A-085EA5386C9A</identifier>
  <sender>NAADS-Testing@NAADS@PelmorexCommunications(Testing)</sender>
  <sent>2011-06-22T06:08:09+00:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <code>profile:CAP-CP:0.3</code>
  <info>
    <language>en-CA</language>
    <category>Met</category>
    <event>Tornado</event>
    <responseType>None</responseType>
    <urgency>Immediate</urgency>
    <severity>Extreme</severity>
    <certainty>Observed</certainty>
    <eventCode>
      <valueName>profile:CAP-CP:Event:0.3</valueName>
      <value>tornado</value>
    </eventCode>
    <expires>2011-06-23T13:00:00+00:00</expires>
    <senderName>Pelmorex Communications (Testing)</senderName>
    <headline>Sample alert with Digital signature </headline>
    <area>
      <areaDesc>Test NAADS signature</areaDesc>
      <polygon>51.552994,-99.216119 51.564488,-99.219607 51.575448,-99.219861 51.576326,-99.221583
51.559342,-99.225395 51.552488,-99.236193 51.538291,-99.244281 51.529917,-99.245778
51.528724,-99.256742 51.523192,-99.261972 51.516722,-99.263953 51.510717,-99.263414
51.507501,-99.265974 51.504579,-99.265929 51.502849,-99.263657 51.498802,-99.26395
51.497321,-99.266635 51.49194,-99.264386 51.490075,-99.266247 51.479374,-99.262484
51.473999,-99.265706 51.474256,-99.204523 51.503636,-99.204828 51.503875,-99.193096
51.532352,-99.192697 51.535124,-99.19768 51.537876,-99.19726 51.553234,-99.202605
51.549832,-99.209311 51.548486,-99.207949 51.543643,-99.210667 51.545245,-99.215015
51.551858,-99.217815 51.551197,-99.215461 51.552994,-99.216119</polygon>
      <geocode>
        <valueName>profile:CAP-CP:Location:0.3</valueName>
        <value>4619068</value>
      </geocode>
    </area>
  </info>
</alert>
```

### 2. Alert Message with digital signature

```
<?xml version="1.0" encoding="UTF-8"?>
<alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>CE1336F2-24ED-5A25-93A4-1F3C4ACA071E</identifier>
  <sender>NAADS-Testing@NAADS@PelmorexCommunications(Testing)</sender>
  <sent>2011-06-22T06:14:25+00:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
```

[illegible]

```

4TNIjYknk77ODTvXSDOIQ/SxcXRbkAstT6R9GuERzFrTLHU8DhYETHhPiRwi1R4xU05tzVy6Sxt4O1JHsY3O
V8npBnfF6ErG1U1SH6FWiYu9S5c8JDeheit75TwYV49R+RlaxEMCAwEAAaOB6DCB5TAJBgNVHRMEAjAAM
EQGA1UdIAQMDSwOQYLIZIAYb4RQEHFwEwkjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVyaXNp
Z24uY29tL3JwYTBALBgNVHQ8EBAMCBaAwHQYDVR0IBBYwFAYIKwYBBQUHAWQCcGAQUFBwMCMBQG
CmCGSAGG+EUBBgCEBhYETm9uZTBQBgNVHR8ESTBHMEWgQ6BBhj9odHRwOi8vaW5kYzFkaWdpdGFsa
WQZzZmY3J3LnZlcm1zaWduLmNvbS9JbmRDMURpZ210YWxJRC1HMy5jcmwwdQYJKoZIhvcNAQEFBQAD
ggEBAD3o5bsnBvkF5zkd1A+nEf3yXOJPhjWTzswwkIAFSwo1FiDcRpBzd98+SjBFs7hG2VuP+5qxudLxCP2
vC6x8HnQAXjmSPx1d95V8UUK0SLaABSHNri85AalpQR4R7t9Vr2hrY0F0T7ft0IvclaRu0B4zUX4uHYFYyuI
9knyJtomAb4HyVSeKpXA4fg87bFK3h94z9p4+l+44nSWia1MKrpQarjQj9TCxZgHN1JEMQtpWNEWeRS+p
g4rymNHvq9ZvYOEQ6LXWgVuqzUB1rFIntQxIGH4gzIso4mOZVqyTQ8cZDp0CFQh7WUIroZyruOlvd8+erZ
CijYVjeXtotwESCgY=
```

```

</X509Certificate>
</X509Data>
</KeyInfo>
<Object xmlns="">
  <SignatureProperties>
    <SignatureProperty Id="NAADS-DSS1" Target="http://dss1-staging.naad-adna.pelmorex.com">
      <xc:value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd"/>
    </SignatureProperty>
    <SignatureProperty Id="NAADS-DSS2" Target="http://dss2-staging.naad-adna.pelmorex.com">
      <xc:value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd"/>
    </SignatureProperty>
  </SignatureProperties>
</Object>
</Signature>
</alert>

```

### 3. DSS Verification Request (SOAP Request on https)

To verify a signed alert, a SOAP request on https must be made to the DSS server as identified in the Signature Property Target of the signed message. The method that must be called is DSSVerifySignedNaadsAlert. The following request must be passed as string parameter.

The request below follows the OASIS-DSS specification. The request ID is used to identify the request from LMD. This should be unique for each request and should have a way to identify the requestor. NAADS will include this Request ID in the response. The document ID will be a unique ID for each specific alert that is being verified and the same ID needs to be repeated in the WhichDocument field under OptionalInputs part of the Verify Request.

Under the Document Id, the entire signed alert that is to be verified is to be provided by the LMD.

```

<VerifyRequest RequestID="0822D9A5-B7B0-0EFB-47F6-A47F2EF12347"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://www.docs.oasis-
open.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd" Profile="">
  <InputDocuments>
    <Document ID="0822D9A5-B7B0-0EFB-47F6-A47F2EF12347">
      <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
        <identifier>0822D9A5-B7B0-0EFB-47F6-A47F2EF12347</identifier>
        <sender>NAADS-Testing@NAADS@PelmorexCommunications(Testing)</sender>
        <sent>2011-06-24T05:38:35+00:00</sent>
        <status>Actual</status>
        <msgType>Alert</msgType>
        <scope>Public</scope>
        <code>profile:CAP-CP:0.3</code>
        <info>
          <language>en-CA</language>
          <category>Met</category>
          <event>Tornado</event>
          <responseType>None</responseType>
          <urgency>Immediate</urgency>
          <severity>Extreme</severity>
          <certainty>Observed</certainty>

```

```
<eventCode>  
<valueName>profile:CAP-CP:Event:0.3</valueName>  
<value>tornado</value>  
</eventCode>  
<expires>2011-06-25T13:00:00+00:00</expires>  
<senderName>Pelmorex Communications (Testing)</senderName>  
<headline>Sample alert with Digital signature</headline>  
<area>  
<areaDesc>Crane river Manitoba</areaDesc>  
<polygon>51.552994,-99.216119 51.564488,-99.219607 51.575448,-99.219861 51.576326,-99.221583  
51.559342,-99.225395 51.552488,-99.236193 51.538291,-99.244281 51.529917,-99.245778  
51.528724,-99.256742 51.523192,-99.261972 51.516722,-99.263953 51.510717,-99.263414  
51.507501,-99.265974 51.504579,-99.265929 51.502849,-99.263657 51.498802,-99.26395  
51.497321,-99.266635 51.49194,-99.264386 51.490075,-99.266247 51.479374,-99.262484  
51.473999,-99.265706 51.474256,-99.204523 51.503636,-99.204828 51.503875,-99.193096  
51.532352,-99.192697 51.535124,-99.19768 51.537876,-99.19726 51.553234,-99.202605  
51.549832,-99.209311 51.548486,-99.207949 51.543643,-99.210667 51.545245,-99.215015  
51.551858,-99.217815 51.551197,-99.215461 51.552994,-99.216119</polygon>  
<geocode>  
<valueName>profile:CAP-CP:Location:0.3</valueName>  
<value>4619068</value>  
</geocode>  
</area>  
</info>  
<Signature Id="NAADS Signature" xmlns="http://www.w3.org/2000/09/xmldsig#">  
<SignedInfo>  
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>  
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>  
<Reference URI="">  
<Transforms>  
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>  
</Transforms>  
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>  
<DigestValue>u+wAlHg+nmiuW/UzDBypGdvpXHo=</DigestValue>  
</Reference>  
</SignedInfo>  
<SignatureValue>BbHbaLc4/iEHRPW//uUMJqIHebDWNURWA3hRS1Bsn7inG5F8Q1X2vWLou9ITzeV4/Z  
FEHGcyC10k0layIPdaUtD07onMXIKXHP626iT99lgMwAuh5G03IQ/t/N0fhac61u8wl6ZUNmUyPeNqdK7NSI  
LrZjYdv7Oq6Lu0/6oBpfQNDbQINVB49CvrAVVY7iaJSVP5bkZqDhlGLBWm3LMlMyk2IJzFPVJE6Va7OGVRhd  
MaaOH0OPA7MKn+6yybewGRBOekVL3epI8PLMUxxSGEF53juqX4DJCNbtbTE/Ib8TNjkcvIttO1D35wWF  
2bckyd10oqrdbJ98ox96xz3Nkw==</SignatureValue>  
<KeyInfo>  
<X509Data>  
<X509Certificate>MIIFazCCBFogAwIBAgIQBO1UglUDPqqRrvrn+2JTANBgqhkiG9w0BAQUFAADCB3TELMAKGAIUEBHMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMRswHQYDVQQLEZXWZXRpU2lnbiBUcnVzdCBOZR3b3JrMTswOQYDVQLZezJUZXJtcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cudmVyaXNPZ24uY29tL3JwYSAAoyYkwOTEeMBWGAIUECxMVUGVyc29uYSBoB3QgVmFsaWRhdGVkMTcwNQYDVQQDEy5WZXJPu2lnbiBDdBGFzcysAxIEluZGl2aWR1YWwgU3Vic2NyaWJlciBIDQSAteEcMB4XDTEExMDUwMzAwMDAwMFoXDTEyMDUwNTIzNTk1OVowdgEYMRCwFYDVQKEw5WZXRpU2lnbiwgSW5jLjEfMb0GA1UECxMWVVmVyaVNpZ24gVHJ1c3QgTmV0d29yazFGMEQA1UECXm9d3d3LnZlcmliZWduLmNvbS9yZXBCvc2l0bzJlSlJlJQQSBjbmNvcnAuIGJ5IFJIZi4sTEIBQi5MVEQoYyk5ODEeMBWGAIUECxMVUGVyc29uYSBoB3QgVmFsaWRhdGVkMTwMMQYDVQQLZEpEaWdpdGFsfGEIEIEIENSYNXnzIDEgLSBOZRzY2FwZSBGbWxsIFNlcnZpY2UxGzAZBgNVBAMUEk5BQURTIERTUyBQZWxtb3JleDeIMCAGCSqsGSib3DQEJARyTbmVob3BzQHBlbg1vcnV4LmNvbTCCA SIwDQYJKozIhvcNAQEBBQADggEPADCAQAoCggEBAK30SDHFqHh9MnB0pzoBBRVck/7XLbyDjREb++ky/+K9eoIdwpH4UIo9HRFLq6WAUjsq24082PysoFk4j13ICOW4bhbfhf2k47e5BQGR+/sgEOkNLziSg2I/2XErMt0+Yb/ZtMGL5Gdnr+YNunlyahdhWQdA4Sefio++r3I3TGRyw9cbhyi0xhhfFdwfr/rOlclRrIrweiqMA34TNijYknk77ODTvXSDOI/Q/SxcXRBkAstT6R9GuERzFrTLHU8DhYETHhpPiRwi1R4xU05tzVy6Sxt401JHSY30V8npbnf6ErG1U1SH6fWiYu9S5c8JDheit75Twyv49R+rlaxEMCAWEAAaOB6DCB5TAJBGNVHRMEAajAAMEQA1UdIAQMDSbwOOYLIZiyAB4RCEHFwEwkJAObggrBgEFBQCARYcaHR0cHM6Ly93d3cudmVyaXNPZ24uY29tL3JwYTALBgNVHQBzEBAMBAwHQYDVROIBBYwFAYIKwYBBQUHAwwGCCsGAQUFBwMCMCBQG CmCGSAGG+EUBBGcEBHYETm9uzTBQBgNVHR8ESTBHMEWgQ6BBhj9odHRWOi8vaW5kYzFkaWdpdGFsa WQtZzMtY3JsLnZlcmliZWduLmNvbS9jbmRDMDURpZ2l0YWwxJCRC1HMY5jcmmwdDYJKozIhvcNAQEFBQAD ggEBAD3o5bsnbvkf5zkdl+aEf3yxOJPhjWTzswwklAFSwo1FiDRcpBzd98+SjBFs7hg2VuP+5qxudLxCp2 vC6x8HnAQ4xjmSPx1d95V8UUokSLAABSHNQR4R7t9Vr2hrYoarOT7ftOIvlaRu0B4zuUX4uHYFYyuI 9knyJtomAbAXHyVsEKpXA4fg87BFK3h94znP4+l+44nsWia1MKRpQarfQj9TCxZgHN1JEMOtPWNEWERs+p
```



```

g4rymNHvq9ZvYOEQ6LXWgVuqzUB1rFIntQxIGH4gzIso4mOZVqyTQ8cZDp0CFQh7WUIroZyruOlvD8+erZ
CijYVjeXtotwESCgY=</X509Certificate>
</X509Data>
</KeyInfo>
<Object xmlns="">
<SignatureProperties>
<SignatureProperty Id="NAADS-DSS1" Target="http://dss1-staging.naad-adna.pelmorex.com">
<xc:Value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd"/>
</SignatureProperty>
<SignatureProperty Id="NAADS-DSS2" Target="http://dss2-staging.naad-adna.pelmorex.com">
<xc:Value xmlns:xc="http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd"/>
</SignatureProperty>
</SignatureProperties>
</Object>
</Signature>
</alert>
</Document>
</InputDocuments>
<OptionalInputs>
<SignaturePlacement WhichDocument="0822D9A5-B7B0-0EFB-47F6-A47F2EF12347"
CreateEnvelopedSignature="true"/>
</OptionalInputs>
<SignatureObject>
<SignaturePtr WhichDocument="0822D9A5-B7B0-0EFB-47F6-A47F2EF12347" XPath="//cs:Signature[Id =
'NAADS Signature']">
</SignaturePtr>
</SignatureObject>
</VerifyRequest>

```

#### 4. DSS Verification Response – Verification Success (SOAP response on https)

NAADS DSS will return the following response over SOAP (as string) as a return value. The ResultMajor field will be success if the message verified successfully and will be ResponderError if the message did not verify successfully.

```

<VerifyResponse RequestID="0822D9A5-B7B0-0EFB-47F6-A47F2EF12347" Profile=""
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://www.oasis-
open.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd">
<Result>
<ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:Success</ResultMajor>
<ResultMinor />
<ResultMessage />
</Result>
</VerifyResponse>

```

#### 5. DSS Verification Response Failed

```

<VerifyResponse RequestID="0822D9A5-B7B0-0EFB-47F6-A47F2EF12347" Profile=""
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns="http://www.oasis-
open.org/dss/oasis-dss-1.0-core-schema-cd-02.xsd">
<Result>
<ResultMajor>urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError</ResultMajor>
<ResultMinor>urn:oasis:names:tc:dss:1.0:resultminor:GeneralError</ResultMinor>
<ResultMessage />
</Result>
</VerifyResponse>

```

NAADS DSS will return a value in ResultMessage (apart from error shown in sample above) if there is some error in the request or XML as follows:

1. Wrong DSS request format  
The XML document is incorrect!
2. Wrong alert format in Verify Request  
The XML document provided is not a signed alert!
3. The alert received doesn't have a "NAADS Signature" element  
The alert wasn't signed by NAADS!

If the request/alert is correct, but the alert cannot be verified (i.e. digital signature did not verify) error will be returned in ResultMajor and Minor as in sample above. The ResultMessage will be blank.

#### **6. Process to validate the digital signature, using a NAAD public key without connecting to the DSS SOAP server**

LMDs with embedded systems (i.e. with no access to the internet) receiving CAP alerts by satellite can validate alerts by running **OpenSSL** commands (Secure Sockets Layer).



It is strongly advised that LMDs register on Pelmorex Public Alerting website (<https://alerts.pelmorex.com/register/>) so they can get the updated certificate information.



## Appendix 5: Sample EC Alert

Following is a SAMPLE of an EC Alert (Please note this is a SAMPLE only and has been modified to fit as the content of this document. This alert will not validate):

```
<?xml version="1.0" encoding="UTF-8" ?>
- <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>2.49.0.1.124.b29ebdf5.2012</identifier>
  <sender>cap@ec.gc.ca</sender>
  <sent>2012-07-06T08:46:53-00:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <source>Environment Canada - Environnement Canada - Toronto
(CWTO)</source>
  <scope>Public</scope>
  <restriction />
  <addresses />
  <code>profile:CAP-CP:0.4</code>
  <code>layer:EC-MS-CMC:1.0</code>
  <code>layer:SOREM:1.0</code>
  <note />
  <references />
  <incidents />
- <info>
  <language>en-CA</language>
  <category>Met</category>
  <event>high heat and humidity</event>
  <responseType>Monitor</responseType>
  <urgency>Future</urgency>
  <severity>Moderate</severity>
  <certainty>Likely</certainty>
  <audience>General Public</audience>
- <eventCode>
  <valueName>profile:CAP-CP:Event:0.4</valueName>
  <value>heatWave</value>
</eventCode>
- <eventCode>
  <valueName>SAME</valueName>
  <value>DMO</value>
</eventCode>
  <effective>2012-07-06T08:46:00-00:00</effective>
  <expires>2012-07-07T00:46:00-00:00</expires>
  <senderName>Environment Canada</senderName>
  <headline>high heat and humidity warning</headline>
  <description />
  <instruction>"Please monitor for further updates to this alert."</instruction>
  <web>http://www.weatheroffice.gc.ca/warnings/warnings_e.html</web>
  <contact />
- <parameter>
```

```

    <valueName>layer:EC-MSC-SMC:1.0:Alert_Type</valueName>
    <value>warning</value>
  </parameter>
- <parameter>
    <valueName>layer:EC-MSC-SMC:1.0:Broadcast_Intrusive</valueName>
    <value>no</value>
  </parameter>
- <parameter>
    <valueName>layer:EC-MSC-SMC:1.0:Parent_URI</valueName>
    <value>msc/alert/environment/hazard/mfile-1.0-ascii/decoded_consolidated-
xml-
2.0/20120706084600000/ww_10_70_cwul/hhw/ww_10_70_cwul_20120706084
6_hhw/public/2012_83526/non-
bi/en_upper_preliminary/fr_not_present</value>
  </parameter>
- <parameter>
    <valueName>layer:EC-MSC-SMC:1.0:CAP_count</valueName>
    <value>34299</value>
  </parameter>
- <area>
    <areaDesc>Metro Montréal - Laval</areaDesc>
    <polygon>45.3667,-73.55 45.3333,-73.7833 45.3487,-73.8063 45.3488,-73.8065
45.3889,-73.8366 45.405,-73.9709 45.481,-74.0046 45.5325,-73.9026 45.534,-
73.8997 45.6168,-73.8331 45.6654,-73.7524 45.6656,-73.7522 45.6662,-73.7511
45.7,-73.632 45.7164,-73.4688 45.7255,-73.4378 45.7207,-73.427 45.5,-73.3667
45.4999,-73.3667 45.4333,-73.4 45.4332,-73.4003 45.369,-73.5447 45.3667,-
73.55</polygon>
  </area>
- <geocode>
    <valueName>layer:EC-MSC-SMC:1.0:CLC</valueName>
    <value>032400</value>
  </geocode>
- <geocode>
    <valueName>profile:CAP-CP:Location:0.3</valueName>
    <value>2458007</value>
  </geocode>
</info>
- <Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="Environment
Canada">
- <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
- <Reference URI="">
- <Transforms>
    <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature" />
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>5vp71PoJwex9R3VQhDsdlnV/7AA=</DigestValue>
</Reference>

```

```

</SignedInfo>
<SignatureValue>ENNOVHCPHuX9PfXxBTeSZtzxVLf9OWbiknBLtvNsXThsGxKdCaB6
B7fXnIT8NJxX
f0MzohQ1Fw0AiEDF4UIOZsqeb53oJOxr08oouYmErJ9pwJX53ANyK5q6XJALUeO4
QonClqBkg0P/11krsLJSDcIESNSBCETmj6fhZSn0EY+tWZEv59K0vfMiqRT1OGf4
w/F//aZ6674yOkIWSaAK3BGxU8aSwnEVA6CN7rjYv61y9kqB7GiWZkrdx8pF6YQw
m2StXM1ph4J/W6ZXvkF/OIRQQsZLaiYFioPm1a/vaJy5LHebzAkpKxrrSD9czGN9
K9FbqNF5C2BkPGtpeEFLg==</SignatureValue>
- <KeyInfo>
- <X509Data>
  <X509Certificate>MIIE1DCCA7ygAwIBAgIETBpRgDANBgkqhkiG9w0BAQUFADCBsT
ELMAkGA1UEBhMC
VVMxFjAUBgNVBAoTDUUVudHJ1c3QsIEluYy4xOTA3BgNVBAsTMHd3dy5lbnRydXN0
Lm5ldC9ycGEgaXMgaW5jb3Jwb3JhdGVkIGJ5IHJlZmVyZW5jZTEfMB0GA1UECjMw
KGMpIDIwMDkgRW50cnVzdCwgSW5jLjEuMCwGA1UEAxMIRW50cnVzdCBDZXJ0aWw
Zp
Y2F0aW9uIEF1dGhvcml0eSAtIEwxQzAeFw0xMTA1MDkxNTIxMzVaFw0xNTA3MTA
w
MzMxMzZaMIGEMQswCQYDVQQGEwJDQTEPMA0GA1UECBMGUXVIYmVjMREwDwYD
VQQH
EwhHYXRpbmVhdTEbMBkGA1UEChMRSW52aXJvbm1lbnQgQ2FuYWRhMR4wHAYD
VQQL
4e2+3iVoJpS/6PNwliAxxImrnhdZ1iE77PQhpfyrchhYSD4VJs2vjA==</X509Certificat
e>
</X509Data>
</KeyInfo>
</Signature>
</alert>

```

**User Notes:**

---