Canadian Wireless Public Alerting (WPA) C-Interface Specification

CRTC Interconnection Steering Committee (CISC) – Network Working Group (NTWG)

NTWG-TIF033 Consensus Obtained: 2015/03/31 (v1.0), updated 2015/04/21 (v1.1), 2016/03/15 (v1.2), updated 2016/10/18 (v1.3), updated 2018/01/04 (v2.0), updated 2019/02/20 (v2.1) and updated 2019/10/08 (v2.2).

Abstract

This Specification defines the interface between the NAAD System WPA Gateway (NAADS WPA Gateway) and the Canadian Wireless Service Provider Gateway (WSP Gateway) for Wireless Public Alerting (WPA) in Canada.

Acknowledgment

It shall be acknowledged that while this Canadian Wireless Public Alerting (WPA) C-Interface Specification represents a unique document, the Joint ATIS/TIA J-STD-101, CMAS Federal Alert Gateway to CMSP Gateway Interface Specification [Ref 30], provided the WPAS Project Team with a baseline reference document from which this specification was derived.

Foreword

This Canadian Wireless Public Alerting (WPA) C-Interface (Carrier Interface) Specification, version 2.2 dated August 28, 2019 is intended to fulfill the need to interconnect Canada's Wireless Service Providers (WSP) with the National Alert Aggregation and Dissemination (NAAD) System for the purpose of issuing emergency alerts to mobile phones in Canada. It defines the security attributes, call flows and communication protocols necessary to develop and operate WPA in conformance with industry standards and Telecom Regulatory Policy CRTC 2017-91.

Revision History

Date	Version	Description	Editor
2015-03-31	1.0	WPAS C-Interface Specification as finalized through consensus within the CRTC Interconnection Steering Committee (CISC) – Network Working Group (NTWG).	J. Tyler Cashion WPAS Service Development Manager
2015-04-21	1.1	Removal of FIPS 140-2 Compliance Requirement and associated references. Finalized through consensus within the CRTC Interconnection Steering Committee (CISC) – Network Working Group (NTWG).	J. Tyler Cashion WPAS Service Development Manager
2016-03-15	1.2	Correction of Event Codes “pyroclaSurge” and “wildFire” to remain conformant with Common Alerting Protocol-Canadian Profile (CAP-CP) specification. Removal of WPA-C-RQMT-0425. It is operationally problematic and is not in keeping with our Canadian Alerting Procedures/Policies. Update WPA-C-RQMT-2920 with additional sentence to clarify. Finalized through consensus within the CRTC Interconnection Steering Committee (CISC) – Network Working Group (NTWG).	J. Tyler Cashion WPAS Service Development Manager
2016-09-06	1.3	Update Section 6.4.2 Message Queuing with additional language to clarify. Corresponding changes also made to the Annex B Configurable Parameters. Update Section 6.5 to reflect the use of Pre-Shared Key (PSK) in place of x.509 Certificates for Network Encryption. Corresponding changes also made to the Annex B Configurable Parameters. Update Section 6.5.3 to reflect that WSPs shall not validate XML Digital Signatures. Includes removal of requirement 2460. Update Section 8.6.2 Internet Protocol (IP) to recommend the use of IPv6 for all C-Interface communication while IPv4 can be optionally used if there is a technical constraint restricting the use of IPv6.	J. Tyler Cashion WPAS Service Development Manager
2016-10-18	1.3	CRTC Interconnection Steering Committee (CISC) – Network Working Group (NTWG) – NTTF033 Forum Consensus Obtained. Document forwarded for NTWG Consensus in October 2016.	J. Tyler Cashion WPAS Service Development Manager
2017-08-04	1.4	Includes updates to the following sections: Change WPAS to WPA in accordance with Telecom Regulatory Policy CRTC 2017-91. Forward Section 4 Legislative & Regulatory Background. Section 5.2, 5.5 & 6.1 to reflect Testing Policies identified in Telecom Regulatory Policy CRTC 2017-91 and Upset Message Lengths of 600 Characters.	J. Tyler Cashion, (One2Many BV) (editor)
2017-09-01	1.5	Includes acceptance of all changes introduced into the 1.4 version of the document plus additional updates to the following sections: Addition of Normative Reference # 42 Changes to Section 1.2 Purpose Minor Updates to Section 4 Legislative & Regulatory Background Changes throughout the document to reflect Updates and/or Removal of language as it pertains to Secure IP Networking Requirements.	J. Tyler Cashion, (One2Many BV) (editor)

Date	Version	Description	Editor
		Changes throughout the document to more clearly identify the functionalities across the C-Interface including improved consistency for employed terms such as “WPA System Test” Items which require some further discussion are highlighted in red with comments from the Editor	
2017-10-10	1.6	Includes acceptance of all changes introduced into the 1.5 version of the document plus additional updates to the following sections: Section 6 – Reread/Rewrite as appropriate Section 7 - Reread/Rewrite as appropriate Section 8 - Reread/Rewrite as appropriate Section 8 - Addition of a new Table 5 Section 8 – Replace All XML Script Examples with Updated Examples produced by the NAAD System. Items which require some further discussion in the TIF033 Form are highlighted in red.	J. Tyler Cashion, (One2Many BV) (editor)
2017-10-25	1.7	Includes acceptance of all changes introduced into the 1.6 version of the document plus additional updates to the following sections: Section 6 – Reread/Rewrite as appropriate Section 7 - Reread/Rewrite as appropriate Section 8 - Reread/Rewrite as appropriate Section 8 – Update to Table 5 Section 8 – Complete Replacement of all XML Scripts Examples to reflect: • New XML Element “WPAC_deliveryChannel” • New XML Values: o Mandatory Public o Invisible Test Annex B, Configurable Parameters – Additional Parameters	J. Tyler Cashion, (One2Many BV) (editor)
2017-11-17	1.8	Includes acceptance of all changes introduced into the 1.7 version of the document plus additional updates to the following sections: Section 3 Definitions, Acronyms, & Abbreviations - Update Section 6 Technical Requirements – Minor Updates to maintain language and reference consistency throughout document. Section 7 C-Interface Call Flows – Minor Updates to maintain language and reference consistency throughout document. Section 8 NAADS WPA Gateway to WSP Gateway Communication Protocol Requirements and Definition – Minor Updates to maintain language and reference consistency throughout document plus: • Addition of Section 8.2.4 Digital Signature • Replacement of Figure 12: C-Interface Document Object Model • Updates to Tables 9, 10, 11, 13, 14, 15, 17, 18, 19, 21, 23, 24, 25, 26, 27, 28, 30, 31 33 • Addition of Tables 12, 16, 20, 22, 29 • Update to XML Scripts to include Digital Signature	J. Tyler Cashion, (One2Many BV) (editor)

Date	Version	Description	Editor
2017-11-24	1.9	Includes acceptance of all changes introduced into the 1.8 version of the document plus additional updates to the following sections: Section 3 Normative References – Addition of Ref 43 Section 8 NAADS WPA Gateway to WSP Gateway Communication Protocol Requirements and Definition – Update to Definitions and further clarity for elements.	J. Tyler Cashion, (One2Many BV) (editor)
2017-12-21	2.0	• Includes acceptance of all changes introduced into the 1.9 version of the document plus final updates in the following sections: • Section 8 – Minor Update to XML Element Requirements whereby: • WPAC_signature is always Optional (O). • WPAC_geocode sub-element is Conditional (C) in the WPAC-area element for Alert, Update and WPA System Test Messages in that "At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all Alert Messages." • Minor Update to Requirement 2540 • Minor Update to Table 33	J. Tyler Cashion, (One2Many BV) (editor)
2019-02-02	2.1	Includes version changes to remove the requirement to validate an alert message against the Event_Code field prior to issuing a WPA message.	Tim Trytten and Jacob Westfall
2019-02-20		NTWG consensus approved version 2.1.	Tim Trytten and Jacob Westfall
2019-05-07	2.2	Includes version changes to correct schema inconsistencies between document and system implementation. Also includes changes to WPAC_Language element to only have mandatory value of "English and French".	Martin Belanger and Nokia Team
2019-05-13	2.2	Includes additional details on the WPAC_Language element. Also includes updated examples with hexdecimal WPAC identifiers	Martin Belanger and Nokia Team

Table of Contents

Table of Figures

Table of Tables

1 SCOPE, PURPOSE, & APPLICATION

This specification defines the technical interface required for the issuance of wireless public alerts. Originating from the Wireless Public Alerting Service Development and Demonstration Initiative[1], this specification was reviewed and obtained consensus within the Canadian Radio-television and Telecommunications Commission (CRTC) - CRTC Interconnection Steering Committee (CISC) – Network Working Group (NTWG) using the Task Identification Form (TIF) process. The NTWG includes representation from Canada's wireless industry and government public alerting communities.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in IETF RFC 2119, available at http://www.ietf.org/rfc/rfc2119.

1.1 Scope

The scope of this specification is the interface between and is inclusive of the National Alert Aggregation and Dissemination (NAAD) System Wireless Public Alerting (WPA) Gateway and Wireless Service Provider (WSP) WPA Gateway for the purpose of issuing WPA alerts. Any processing in either the NAAD System or the WSP network which is not related to this interface is beyond the scope of this specification. The scope is further bound by conformance with 3rd Generation Partnership Project (3GPP) Technical Specifications for Cell Broadcasting [Ref 36 and 37] and the applicable Canadian alerting standards including the Common Alerting Protocol (CAP) [Ref 4] and has been derived from the Commercial Mobile Alerting System (CMAS) J-STD-101, CMAS Federal Alert Gateway to CMSP Gateway Interface Specification, [Ref 30] which was employed as a reference document.

1.2 Purpose

This specification has been developed to meet Telecom Regulatory Policy CRTC 2017-91 [Ref 42], the requirements issued to date by Canada's Senior Officials Responsible for Emergency Management (SOREM) in regards to the Wireless Public Alerting Service [Ref 31] and the WPAS Requirements Definition [Ref 33] as developed and approved by the WPAS Steering Committee. Modifications to this specification may be required as future relevant requirements are released by SOREM.

The National Alert Aggregation and Dissemination (NAAD) System is the government-mandated national aggregator that collects and validates alerting messages generated using Common Alerting Protocol – Canadian Profile - (CAP-CP) by authorized government authorities for the National Public Alerting System (NPAS). As such, The NAAD System shall provide a logical interface to Canadian WSPs who are mandated to participate in NPAS and disseminate WPA alerts to the public. This

[1] The Wireless Public Alerting Service Development and Demonstration Initiative was a public and private partnership project that developed and demonstrated a cell broadcast and LTE based wireless public alerting solution integrated with the National Public Alerting System. The project was funded through the Canadian Safety and Security Program (CSSP), a federal program led by Defence Research and Development Canada's (DRDC) Centre for Security Science, in partnership with Public Safety Canada. Project partners include Bell Mobility, Pelmorex Media Inc., Office of the Fire Marshal and Emergency Management Ontario, Ontario Power Generation, Public Safety Canada, and Mobility & Wireless Solutions. The project was sponsored and managed by Innovation, Science and Economic Development Canada.

specification defines the interface between the NAAD System WPA Gateway (NAADS WPA Gateway) and the Wireless Service Provider Gateway (WSP Gateway) for the dissemination of WPA alerts in Canada.

1.3 Application

This specification is applicable to Canadian WSPs, the NAAD System operator and organizations that use or govern Canada's National Public Alerting System (NPAS).

2 NORMATIVE REFERENCES

The following standards and references contain provisions that, through reference in this text, constitute provisions of this Canadian Wireless Public Alerting (WPA) C-Interface Specification. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this specification are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Where there may be discrepancies in the standards and references below, the Canadian references shall prevail over the other references.

[Ref 1] IETF RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1*; June 1999.[2]

[Ref 2] IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*; January 2005.[1]

[Ref 3] IETF RFC 4301, *Security Architecture for the Internet Protocol*; December 2005.[1]

[Ref 4] *Common Alerting Protocol, v. 1.2; OASIS Standard CAP-V1.2*; July 2010.[3]

[Ref 5] Federal Information Processing Standards Publication 180-3, *Secure Hash Standard; National Institute of Standards and Technology (NIST)*; October 2008.[4]

[Ref 6] IETF RFC 2141, *URN Syntax*; May 1997.[1]

[Ref 7] IETF RFC 4303, *IP Encapsulating Security Payload (ESP)*; December 2005.[1]

[Ref 8] IETF RFC 4306, *Internet Key Exchange (IKEv2) Protocol*; December 2005.[1]

[Ref 9] IETF RFC 4305, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*; December 2005.[1]

[Ref 10] IETF RFC 3715, *IPsec-Network Address Translation (NAT) Compatibility Requirements*; March 2004.[1]

[Ref 11] IETF RFC 4158, I*nternet X.509 Public Key Infrastructure: Certification Path Building*; September 2005. [1]

[Ref 12] IETF RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*; September 2003.[1]

[Ref 13] IETF RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*; November 1998. [1]

[Ref 14] IETF RFC 3447, *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*; February 2003.[1]

[Ref 16] IETF RFC3275, *(Extensible Markup Language) XML-Signature Syntax and Processing*; March 2002.[1]

[Ref 17] IETF RFC793, *Transmission Control Protocol*; September 1981. [1]

[Ref 18] IETF RFC 1122, *Requirements for Internet Hosts -- Communication Layers*; October 1989.[1]

[Ref 19] IETF STD 5 (RFC 791), *Internet Protocol (IPv4) Specification*; September 1981.[1]

[Ref 20] IETF STD 5 (RFC 792), *Internet Control Message Protocol*; September 1981.[1]

---

[2] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[3] This document is available from the Organization for the Advancement of Structured Information Standards (OASIS). < http://www.oasis-open.org/specs/index.php >

[4] This document is available from the National Institute of Technology and Standards (NIST). < http://www.nist.gov/aes >

[Ref 21] IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*; December 1998.[1]

[Ref 22] IETF RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*; December 1998.[1]

[Ref 23] IETF RFC 4291, *IP Version 6 Addressing Architecture*, February; 2006.[1]

[Ref 24] IETF RFC 4443, *Internet Control Message Protocol Version 6 (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*; March 2006.[1]

[Ref 25] IETF RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*; June 1999.[1]

[Ref 26] IETF RFC 4718, *IKEv2 Clarifications and Implementation Guidelines*; October 2006.[1]

[Ref 27] W3C Recommendation, *XML Signature Syntax and Processing, Second Edition*; June 10, 2008.[5]

[Ref 28] NIST SP 800-77, *Guide to IPsec VPNs*; December 2005.[3]

[Ref 29] IETF RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*; May 2007.[1]

[Ref 30] J-STD-101, *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification;* January 30, 2009.[6]

[Ref 31] SOREM Public Alerting Working Group, FPT REQUIREMENTS for WIRELESS PUBLIC ALERTING v. 1.0; May 2013.[7]

[Ref 32] SOREM Public Alerting Working Group, NATIONAL PUBLIC ALERTING SYSTEM COMMON LOOK AND FEEL GUIDANCE[8]

[Ref 33] WPAS Steering Committee, WPAS Functional and Technical Requirements (WPAS Requirements) Definition - Deliverable 1.9; August 2014.[9]

[Ref 34] Public Safety Canada, Request to CISC to develop technical specifications for a wireless public alerting service, July 2014.[10]

[Ref 35] CRTC Decision, Broadcasting Regulatory Policy CRTC 2014-444-Section 101, August 2014.[11]

[Ref 36] 3GPP TS 23.041 3RD Generation Partnership Project; Technical Specifications Group Core Network and Terminals; Technical Realization of Cell Broadcast Service (CBS).[12]

---

[5] This document is available from the World Wide Web Consortium (W3C). < http://www.w3.org/TR/xmldsig-core/ >

[6] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS). < http://www.atis.org >

[7] This document is available from Canadian Radio-television and Telecommunications Commission < http://www.crtc.gc.ca/public/cisc/n-docs/NTCO0587.docx >

[8] This document is available from Public Safety Canada. < https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/npas/clf-lng-12-en.aspx >

[9] This document is available from Canadian Radio-television and Telecommunications Commission < http://www.crtc.gc.ca/public/cisc/n-docs/NTCO0582.pdf >

[10] This document is available from Canadian Radio-television and Telecommunications Commission < http://www.crtc.gc.ca/public/cisc/nt/NTOD0012.pdf >

[11] This document is available from Canadian Radio-television and Telecommunications Commission < http://www.crtc.gc.ca/eng/archive/2014/2014-444.htm >

[12] This document is available from < http://www.3gpp.org/DynaReport/23041.htm >

[Ref 37] 3GPP TS 22.268 3RD Generation Partnership Project; Technical Specification Group Services and System Aspects; Public Warning System (PWS) requirements. [13]

[Ref 38] Senior Officials Responsible for Emergency Management (SOREM) Broadcast Immediately (BI) Alert List.

[Ref 39] Canadian Official Languages Act.[14]

[Ref 40] CAP-CP Location References list - Geocode Annex

[Ref 41] Canadian Profile of the Common Alerting Protocol (CAP-CP).

[Ref 42] CRTC Telecom Regulatory Policy CRTC 2017-91 Implementation of the National Public Alerting System by wireless service providers to protect Canadians15

[Ref 43] International Standards Organization (ISO) date and time format - ISO 8601[16]

[13] This document is available from < http://www.3gpp.org/DynaReport/22268.htm >

[14] This document is available from < http://laws-lois.justice.gc.ca/eng/acts/O-3.01/page-1.html >

[15] This document is available from < http://crtc.gc.ca/eng/archive/2017/2017-91.htm >

[16] This document is available from <https://www.iso.org/iso-8601-date-and-time-format.html>

3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS

3.1 Definitions

3.1.1 Alert Message. A complete CAP message, which may encapsulate one or more audience alert messages. See CAP documentation for further clarification [Ref 4].

3.1.2 Audience Alert Message. A complete message within a CAP message, that may be distinct from another audience alert message due to differences in message content, language, targeted geography area, severity, urgency certainty, etc., and which is identifiable within the CAP message as a separate <info> block. It may or may not include audio and or other resources.

3.1.3 Broadcast Delay. The time between the CAP alert message is made available to a last mile distributor and the audience alert message(s) being presented to the public.

3.1.4 Broadcast Immediately (BI) List [Ref 38]. A SOREM defined list of emergency event types with the highest values in urgency, severity and certainty. All events in this list are life threatening and are to be disseminated to the public immediately. WPA shall be employed to only deliver BI Alerts and their associated Update and Cancel messages.

3.1.5 C-Interface (Carrier Interface). The operational interface between and inclusive of the National Alert Aggregation and Dissemination (NAAD) System Wireless Public Alerting Service (WPA) Gateway and Wireless Service Provider (WSP) Gateway for the purpose of issuing WPA alerts.

3.1.6 Canadian Profile of the Common Alerting Protocol (CAP-CP). A set of rules and references specific to the use of CAP in Canada [Ref 41].

3.1.7 Cell Broadcast Centre (CBC). The component within a WSP's Cell Broadcast System that receives and directs the geo-targeted delivery of the Audience Alert Message through the core network to the correct Radio Access Network (RAN) sectors.

3.1.8 Cell Broadcast System (CBS). The components within a WSP's network including the mobile devices (handsets) that are necessary to facilitate the geo-targeted delivery of Cell Broadcast Audience Alert Messages. Sub Components include (but are not limited to) the WSP Gateway, Cell Broadcast Centre (CBC), the LTE communications network, the Radio Access Network (RAN) and Cell Broadcast enabled Mobile Devices.

3.1.9 Common Alerting Protocol (CAP). An international alert message format standard managed by OASIS, the Organization for the Advancement of Structured Information Standards. http://docs.oasisopen.org/emergency/cap/ and refers to Standard CAP-V1.2, July 2010 [Ref 4].

3.1.10 CAP Layer. A specification developed by one or more members of the alerting community that relates to the extension of CAP, in accordance with CAP, for including additional content within a CAP alert message. e.g., A "Broadcast Immediately" element value is defined in the SOREM Layer specification.

3.1.11 CAP Profile. A specification developed by one or more members of the alerting community that includes additional constraints and rules for CAP users, all of which shall be within the bounds of the CAP standard. e.g., Canadian Profile of the Common Alerting Protocol (CAP-CP) [Ref 41].

3.1.12 Common Look and Feel (CLF). The objective of presenting clearly recognizable authoritative audience alert messages to the Canadian public through the diversity of communications media and distributors supporting the NPAS initiative [Ref 32].

3.1.13 Commercial Mobile Alert System. The Commercial Mobile Alert System (CMAS) refers to the American voluntary emergency alerting system. The service is now called Wireless Emergency Alerts (WEA) but the technical specifications for this service are still referred to as CMAS Specifications.

3.1.14 Commercial Mobile Service Provider (CMSP). A Commercial Mobile Service Provider (or CMS Provider) is the American WEA/CMAS equivalent to a Canada Wireless Service Provider (WSP).

3.1.15 Last Mile Distributor (LMD). Operators of technology based service delivery systems that disseminate National Public Alerting System messages (Audience Alert Messages) to the public. LMDs include, but are not limited to, radio, television, Internet, landline or cellular telecommunication, billboard, and other forms of wireline or wireless technology service deliveries or systems. Any party that transmits standardized emergency alerts directly to the public, in a "made for end client" presentation, are LMDs. The LMD is responsible for delivery and presentation of the Alert Message while Alerting Authorities are responsible for the message content.

3.1.16 LTE (Long Term Evolution) Network. Long-Term Evolution (commonly marketed as 4G LTE) is an international standard for wireless communication of high-speed data for mobile phones and data terminals. This is the network technology being used for WPA and is a component within the Cell Broadcast System.

3.1.17 National Alert Aggregation & Dissemination (NAAD) System. The CAP alert message aggregation system recognized as the national aggregator for NPAS. Owned and operated by Pelmorex Communications Inc. The NAAD System also operates the NAADS WPA Gateway.

3.1.18 National Public Alerting System (NPAS). The Canadian federal/provincial/territorial government led public alerting initiative.

3.1.19 Pelmorex Public Alerting Governance Council. The Governance Body from which the National Alert Aggregation & Dissemination (NAAD) System takes direction and receives assistance.

3.1.20 Radio Access Network (RAN). A Radio Access Network (RAN) is part of a mobile telecommunication system. Conceptually, it resides between a device such as a mobile phone, and the core network, which is the LTE Network for WPA. It is often referred to as the Air Interface and it is a component within the Cell Broadcast System.

3.1.21 SOREM. Senior Officials Responsible for Emergency Management (SOREM) is a forum of Federal/Provincial/Territorial (F/P/T) officials responsible for coordinating a strategy for emergency management in Canada, and for providing guidance and advice on how to enhance emergency management in Canada. SOREM includes representatives from provincial and territorial emergency management organizations and Public Safety Canada.

3.1.22 SOREM Layer. A public alerting specification developed and owned by SOREM that provides NPAS specific CAP Layer elements and is defined in the CLF.

3.1.23 Wireless Public Alert Architecture for C-Interface (WPAC). The technical architecture required for the C-Interface and the reliable transmission of WPAMs across the C-Interface from the NAAD System to multiple WSPs.

3.1.24 Wireless Public Alert Message (WPAM). A derivative of an original CAP message info block that has been specifically assembled by the NAADS WPA Gateway for transport across the WPAC for processing by the WSP Gateway.

3.1.25 Wireless Service Provider (WSP). A CRTC and Industry Canada licensee operating their own network and providing mobile voice and data services in Canada.

3.1.26 WSP Gateway. A WSP administered system, identified by a unique IP address or Fully Qualified Domain Name, which interfaces with the NAADS WPA Gateway via the WPAC protocol to process and condition WPAMs for delivery of Audience Alerts via the Cell Broadcast Centre.

3.1.27 WSP Gateway Group. A WSP Gateway Group is the set of WSP Gateways whose IP addresses or Fully Qualified Domain Names are visible to the NAADS WPA Gateway across the C-Interface. A WSP Gateway Group shall consist of one or two WSP Gateways.

3.2 Acronyms & Abbreviations

AES	Advanced Encryption Standard
AH	Authentication Header
ATIS	Alliance for Telecommunications Industry Solutions
BI	Broadcast Immediate
CA	Certificate Authority
CAP	Common Alerting Protocol
CAP-CP	Common Alerting Protocol – Canadian Profile
CBC	Cell Broadcast Centre
CISC	CRTC Interconnection Steering Committee (Canada)
CLF	Common Look and Feel Guidance (Canada)
CMAS	Commercial Mobile Alert System (USA)
CMSP	Commercial Mobile Service Provider (USA)
CRTC	Canadian Radio-television and Telecommunications Commission (Canada)
ESP	Encapsulating Security Payload
FIFO	First In First Out
FQDN	Fully Qualified Domain Name
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	IP Security
MI	Message Identifier
NIST	National Institute of Standards and Technology (USA)
NPAS	National Public Alerting System (Canada)
NTWG	Network Working Group (Canada)
OCSP	Online Certificate Status Protocol
RFC	Request for Comment
RSA	Rivest, Shamir, and Adleman
SA	Security Association
SGC	Standard Geographical Classification
SHA-1	Secure Hash Algorithm One
SOREM	Senior Officials Responsible for Emergency Management (Canada)
TCP	Transmission Control Protocol

TIA	Telecommunications Industry Association
URI	Uniform Resource Identifier
URN	Uniform Resource Name
W3C	World Wide Web Consortium
WPAC	Wireless Public Alert Service Architecture for C-Interface (Canada)
WPAM	Wireless Public Alert Message (Canada)
WPA	Wireless Public Alerting (Canada)
WSP	Wireless Service Provider (Canada)
XML	eXtensible Markup Language

4 LEGISLATIVE & REGULATORY BACKGROUND

The Canadian telecommunication and broadcast industry are governed by policies set out in the Broadcasting Act, Telecommunications Act and Canada's anti-spam legislation (CASL). The Canadian Radio-television and Telecommunications Commission (CRTC) (http://www.crtc.gc.ca/eng/acrtc/acrtc.htm) is the Canadian government regulator who supervises the industries and issues orders and regulations based on the objectives stated in the policies.

In 2009, the CRTC designated a Canadian national public alerting message aggregator (https://alerts.pelmorex.com/) for the National Public Alerting System (NPAS) (http://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/ntnl-pblc-lrtng-sstm-eng.aspx, http://www.crtc.gc.ca/eng/archive/2009/2009-340.htm).

In May 2013, the Federal/Provincial/Territorial (FPT) Public Alerting Working Group of Senior Officials Responsible for Emergency Management produced the "F/P/T REQUIREMENTS for WIRELESS PUBLIC ALERTING v. 1.0" [Ref 31]. This document was developed as a starting point for discussion amongst the wireless industry, Public Safety Canada (PS), Industry Canada, and the CRTC regarding public safety authorities' expectations for wireless public alerting distribution. Also, of note is the National Public Alerting System Common Look and Feel Guidance [Ref 32] released by the F/P/T Public Alerting Working Group in April 2013. Although focused on public alert distribution through television and radio broadcast media, this guidance document provides additional information about the expected user experience for Canadians receiving NPAS alerts via multiple distribution channels. The WPAS Operational and Functional Requirements Definition [Ref 33] was then developed based upon these two preceding documents. This document reflects the required functional and operational requirements for WPA.

In July of 2014, Public Safety Canada issued a Letter of Request to the Chair of the CRTC Interconnection Steering Committee (CISC) to begin developing specifications for WPA [Ref 34]. This was further assigned to CISC's Network Working Group (NTWG) where a Task Information Form (TIF) 033 was opened. The NTWG includes representation from the Canadian Radio-television and Telecommunications Commission (CRTC) as well as Canada's Wireless Service Providers (WSP). The NTWG then endeavoured to develop Canadian WPA Technical Implementation Specifications for both Mobile Devices and Network Integration. This document represents the Network Integration specifications for WPA.

In August 2014, the CRTC issued a Broadcasting Regulatory Policy CRTC 2014-444 and Broadcasting Orders CRTC 2014-445, 2014-446, 2014-447 and 2014-44 [Ref 35]. While these new regulations mandated that Radio and Television outlets must deliver Public Alerts to their listeners and viewers, Section 101 of this Regulatory Policy further states that "Although the Commission is addressing the participation of the broadcasting industry in emergency alerting in the present policy, it strongly encourages, as it did in Broadcasting Decision 2011-438, the use of digital media and mobile platforms to alert Canadians to imminent or unfolding dangers, particularly given the increase since 2011 in the use of mobile devices by Canadians. The Commission notes that Public Safety Canada has requested that the CRTC Interconnection Steering Committee (CISC) initiate a new task to assist in the development of the technical specifications and network design of a wireless public alerting service for Canada. Subsequently, the Defence Research and Development Canada Centre for Security Science, through the Canadian Safety and Security Program, will implement a pilot project based on the technical specifications and a network design developed by CISC, to build, test and operate an effective wireless public alerting service. The Commission awaits the results of these initiatives." It was

anticipated that WPA would also be included in the regulatory landscape of Canada's NPAS in the future.

On April 29, 2015, the CRTC announced in their 3-Year Plan that for:

- Fiscal Year Ending March 2016 "The CRTC will also monitor the progress of the industry's implementation of the Wireless Public Alerting Service (WPAS) standards stemming from the Communications Interoperability Strategy for Canada."
- Fiscal Year Ending March 2017 "The CRTC will also monitor the wireless carrier industry's developments with respect to the WPAS and a pilot project regarding WPAS implementation. Based on these developments, a public proceeding may be launched on WPAS."
- Fiscal Year ending March 2018 "If a public proceeding regarding WPAS implementation by the wireless industry is required, the CRTC will complete this proceeding, including the establishment of policy guidelines and the implementation of timeframes for industry compliance."

By March 2016, the WPAS Development and Demonstration Initiative successfully completed technical and functional validation. Following this, the CRTC issued Telecom Notice of Consultation CRTC 2016-115 on March 29, 2016 to solicit public comments for the participation by Wireless Service Providers (WSP) in the National Public Alerting System. Concurrently, the WPAS Development and Demonstration Initiative continued to successfully pilot the service in the Regional Municipality of Durham after which the project completed on March 31, 2017. Following the successful WPAS pilot and after receiving more than 200 interventions from interested parties during the consultation, the CRTC issued Telecom Regulatory Policy CRTC 2017-91 [Ref 42] on April 6, 2017 to mandate Canadian WSPs to implement Wireless Public Alerting (WPA) in Canada.

4.1 Key Government of Canada Provisions

Canada is subject to the Official Languages Act [Ref 39], which is a Canadian law that came into force on September 9, 1969 and was substantially amended in 1988. The official languages of Canada are English and French, which "have equality of status and equal rights and privileges as to their use in all institutions of the Parliament and Government of Canada," according to Canada's constitution. Official bilingualism is the term used in Canada to collectively describe the policies, constitutional provisions, and laws that ensure legal equality of English and French in the Parliament and courts of Canada, protect the linguistic rights of English and French-speaking minorities in different provinces, and ensure a level of government services in both languages across Canada.

In addition to the symbolic designation of English and French as official languages, official bilingualism is generally understood to include any law or other measure that:

- mandates that the federal government conduct its business in both official languages and provide government services in both languages;
- encourages or mandates lower tiers of government (most notably the provinces and territories, but also some municipalities) to conduct themselves in both official languages and to provide services in both English and French rather than in just one or the other;
- places obligations on private actors in Canadian society to provide access to goods or services in both official languages (such as the requirement that food products be labeled in both English and French);
- provides support to non-government actors to encourage or promote the use or the status of one or the other of the two official languages. This includes grants and contributions to groups representing the English-speaking minority in Quebec and the French-speaking minorities in the

other provinces to assist with the establishment of an infrastructure of cultural supports and services.

At the provincial level, New Brunswick and Manitoba officially recognize the equal status of French and English. While French has equal legal status in Manitoba restored due to a court ruling that struck down seventy-year-old English-only laws in 1985, in practice, French language services are only provided in some regions of the province. Quebec has declared itself officially unilingual (French only). Alberta and Saskatchewan are also considered unilingual (English only). In practice, all provinces, including Quebec, offer some services in both English and French and some publicly funded education in both official languages up to the high school level (English language postsecondary education institutions are also present in Quebec, as are French language postsecondary institutions in other provinces, in particular in Ontario and New Brunswick). English and French are official languages in all three territories.

As such, the WPA platform including the C-Interface shall be architected to deliver bilingual alerts. Furthermore, it shall be architected to leave the choice of language and the sequence of language to be the responsibility of the Alerting Authorities. These could include English unilingual, French unilingual, English plus French bilingual or French plus English bilingual alerts depending upon the region being geo-targeted for an emergency alert.

5 REFERENCE ARCHITECTURE

5.1 General C-Interface System Requirements

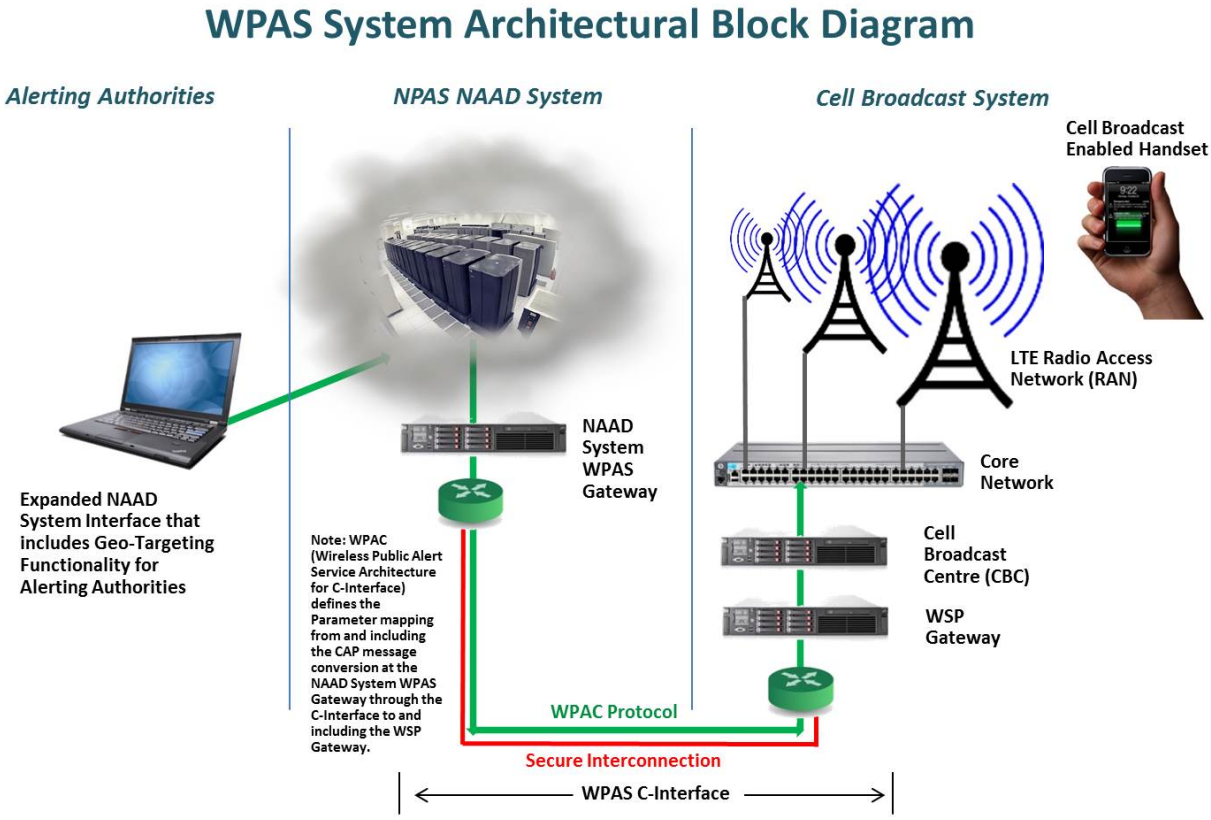

Figure 1: WPA Reference Architecture

5.2 WPA C-Interface

The WPA C-Interface represents the physical and communication protocol interconnection between the NAADS WPA Gateway and the WSP Gateway. The WPA C-Interface:

1. Provides information for the authentication and validation of actions across this reference point.
2. Supports delivery by the NAADS WPA Gateway of a new or updated Wireless Public Alert Message (WPAM) across the Wireless Public Alert Service Architecture for C-Interface (WPAC) to the WSP Gateway in the Cell Broadcast System (CBS).
3. Supports delivery of a cancellation WPAM by the NAADS WPA Gateway whereby the cancellation WPAM terminates the ongoing broadcasting of an associated alert message on the CBS prior to the WPAM's expiry time.
4. Supports delivery of a System Test Message (also a WPAM) by the NAADS WPA Gateway whereby the test WPAM is delivered by the CBS using the WPA System Test Channel (MI=4380).

5. Provides acknowledgement from the WSP Gateway to the NAADS WPA Gateway that the Alert Message, Updated Message, Cancelled Message or WPA Test Message WPAM has been received by the WSP Gateway.
6. Provides periodic C-Interface Link Testing to confirm ongoing connectivity and availability.

Regarding the choice of protocol over the C-Interface, it was concluded that the Common Alerting Protocol – Canadian Profile (CAP-CP) should be terminated at the NAADS WPA Gateway, and a new protocol be defined across the C-Interface. One of the primary considerations for terminating the CAP-CP protocol is that CAP-CP is not suitable to be sent to the mobile devices. The CAP protocol can contain hundreds if not thousands of characters of text while the technology to broadcast messages within the CBS is technology constrained to much shorter message lengths. The CAP-CP protocol also does not support all the functions envisioned over the C-Interface such as a "Link Test", "Acknowledgement (Ack)" and "Error" messages.

Given these considerations, the recommendation (as similarly adopted by CMAS [Refs 9, 22, & 24]) was to develop a new protocol over the C-Interface and terminate the CAP-CP protocol at the NAADS WPA Gateway. This protocol is referred to as the Wireless Public Alert Service Architecture for C-Interface (WPAC).

The WPAC is primarily used to deliver the Wireless Public Alert Message (WPAM) from the NAADS WPA Gateway to the WSP Gateway. The WPAM is an XML file that includes all of the information necessary for the CBS to process and deliver the alert or test messages.

The NAADS WPA Gateway will determine if a WPAM will be generated based upon criteria contained in the corresponding CAP-CP Alert Message. Furthermore, the WPAM shall be constructed from some of the information elements contained within the corresponding CAP-CP message. Every WSP will receive the identical WPAM.

5.3 NAADS WPA Gateway

The alert origination side of the C-Interface is the NAADS WPA Gateway. The functions and requirements to be performed by the NAADS WPA Gateway are defined in Section 6.2, *NAADS WPA Gateway Requirements* and in Section 6.4, *Quality of Service Requirements*. The NAADS WPA Gateway is a functional entity that may be implemented across multiple physical entities.

5.4 WSP Gateway

On the WSP side of the C-Interface is the WSP Gateway. The functions and requirements to be performed by the WSP Gateway are defined in Section 6.3, *WSP Gateway Requirements*. The WSP Gateway is a functional entity that may be implemented across multiple physical entities.

5.5 WPA System Testing

WPA System Testing provides a means to verify and validate the operations of the WPA System.

5.5.1 WPA System Test

WPA System Tests shall be delivered over the WPA System Test Channel (MI=4380) by the CBS to the geo-targeted area(s) identified in the WPAM. The WPA System Test can be used to test the latency, geo-targeting accuracy, message integrity, and overall performance of the WPA system. WSPs shall participate in scheduled WPA system tests.

Mobile devices supporting WPA are not required to support reception of the WPA System Test Messages. Accordingly, WSPs shall not be required to deliver WPA System Test information to subscriber handsets. However, WSPs shall provide one or more mobile devices with the capability for receiving the WPA System Test Messages for testing purposes.

NOTE: Mobile devices with the capability of receiving WPA System Test Messages are subject to WSP policy and the capability is beyond the scope of this Specification.

NOTE: NPAS Public Awareness Tests may be delivered as actual Alert Messages over the WPA Mandatory Reception Channel (MI=4370) or as WPA System Test Messages over the WPA System Test Channel (MI=4380). This will be determined in the NAADS WPA Gateway. See Annex C NPAS Public Awareness Tests – WPA Considerations

5.5.2 C-Interface Link Test

There shall be regular testing on the C-Interface to ensure the ability of the NAADS WPA Gateway and the WSP Gateway can communicate with one another.

6 TECHNICAL REQUIREMENTS

This section defines the requirements for the interface between the NAADS WPA Gateway and the WSP Gateway. These requirements are intended to meet the WPAS Functional and Technical Requirements Definition [Ref 33], the National Public Alerting System Common Look and Feel Guidance [Ref 32], the CRTC issued Telecom Regulatory Policy CRTC 2017-91 [Ref 42] and are grouped as follows:

- General C-Interface system requirements
- NAADS WPA Gateway requirements
- WSP Gateway requirements
- Quality of Service requirements
- Security requirements
- WPA System Test requirements

The requirements defined in this *Section 6, Technical Requirements* and *Section 8, NAADS WPA Gateway to WSP Gateway Communication Protocol Requirements and Definition* shall serve as the basis for testing the NAADS WPA Gateway to WSP Gateway interface.

6.1 General C-Interface System Requirements

The following are general C-Interface system requirements. The specific interface requirements to meet these general system requirements are contained in the remainder of this Specification.

1. The NAADS WPA Gateway and the WSP Gateway shall support the defined WPA C- interface and associated protocols.
2. The C-Interface shall support the ability for the NAADS WPA Gateway to interface with multiple WSPs and to provide interfaces to two or more WSP Gateways per WSP.
3. The C-Interface shall support geographically redundant NAADS WPA Gateway and WSP Gateway deployments in order to avoid a single point of failure.
4. Each WSP Gateway on the C-Interface, whether deployed in redundant or geo-redundant configuration, shall be uniquely identified to the NAADS WPA Gateway by a unique IP address or Fully Qualified Domain Name.
5. A WSP Gateway shall have the capability to temporarily disable the transmission of all Wireless Public Alert Messages (WPAMs) on the C-Interface from the NAADS WPA Gateway to the WSP Gateway. While WPAM delivery to WSP Gateway has been stopped, the NAADS WPA Gateway shall establish an alert queue for the specific WSP Gateway.
6. The administrator of the NAADS WPA Gateway shall establish a process whereby an authorized WSP representative can provide notification of a planned or unplanned outage of a WSP Gateway. During that outage period, WPAMs are not delivered from the NAADS WPA Gateway to that specific WSP Gateway over the C-Interface.
7. The support of a bilingual (English and French) WPAM is required by the Official Languages Act [Ref 39]. However, to address the potential need to deliver alerts in languages other than English and French, the C-Interface shall have the capability to be enhanced in the future to support additional languages.
8. For future WPA capability, the C-Interface may support the capability for the WSP Gateway to retrieve any resources (e.g., audio, video, multimedia files such as graphics) from the NAADS

WPA Gateway if the alert attributes indicate a resource is available.[16]

6.1.1 NAADS WPA Gateway Considerations

These NAADS WPA Gateway considerations are only those that are relative to the interface with the WSP Gateway (i.e., the C-Interface).

1. The NAADS WPA Gateway shall generate WPAMs derived from the originating CAP-CP messages and as generated by Alerting Authorities. The NAADS WPA Gateway will then forward the WPAMs to the WSP Gateway using the C-Interface protocol defined in this Specification.
2. The NAADS WPA Gateway shall combine the French and English language alert text in the originating CAP-CP message into a single bilingual text field within the WPAM that is then forwarded to the WSP Gateway for transmission by the CBS to mobile devices.
3. The NAADS WPA Gateway shall provide a C-Interface transmission control mechanism to buffer the WPAM traffic upon receiving an overload warning from the WSP Gateway.
4. The NAADS WPA Gateway shall only create and send WPAMs over the C-Interface which meet the requirements for BI Alert Messages and associated Update or Cancel Messages.
5. The NAADS WPA Gateway shall include in the WPAM the alert geographic targeting information to provide the CBS with the information needed to transmit the alert message to the corresponding cellular coverage area within the WSP's network. WSPs shall make the best effort to broadcast to the cellular sectors for which the coverage area intersects with the indicated alert area.

   NOTE: Due to RF propagation and location of cell sites, the area where the WPA message is broadcast is only a best approximation of the defined alert area. The actual WPA broadcast will likely exceed or possibly not fully cover the alert area depending on WSP network coverage areas.

6.1.2 WSP Gateway Considerations

1. The WSP Gateway shall provide secure, redundant, and reliable connections to receive WPAMs across the WPAC from the NAADS WPA Gateway. Each WSP Gateway, whether deployed in a simplex or redundant configuration, shall be identified by a unique IP address or Fully Qualified Domain Name.
2. The WSP Gateway shall authenticate interactions with the NAADS WPA Gateway and validate WPAC message integrity and parameters. The WSP Gateway shall provide an error message immediately to the NAADS WPA Gateway if a validation fails.
3. The WSP Gateway shall not perform any formatting, reformatting, or translation of an Alert Message, except for transcoding a text, audio, video, or multimedia file[17] into the format supported by mobile devices.
4. The WSP Gateway shall process the geo-targeting information contained within the WPAM so that the CBS can map the Alert Message to an associated set of transmission sites.
5. The WSP Gateway shall support a mechanism on the C-Interface with the NAADS WPA Gateway to stop and start alert message deliveries from the NAADS WPA Gateway to the WSP Gateway under such conditions that too many messages are being received on the interface, the WSP Gateway buffers are full, congestion exists at the WSP Gateway, etc. Once the condition that requires ceasing transmission has cleared, the WSP Gateway shall notify the NAADS WPA

[17] This release of this specification is limited to text only WPA alert messages. The support of audio, video, and multimedia files is for future study.

Gateway to restart WPAM delivery over the WPAC and retry delivery of WPAMs in the queue if the WPAMs have not expired.

6. The WSP Gateway shall process an Alert Message on a first in–first out (FIFO) basis.
7. The WSP Gateway may reject WPAMs received over the C-Interface that do not meet WPA Alert Message requirements. Specifically, WPAMs may be rejected if:
   - The WPAM does not contain the parameters required by the WSP to perform geographic targeting;
   - The WPAM doesn't include an expiry time; and
   - The WPAM text field contains less or more characters than is permitted by the Cell Broadcast Technology or is defined in the National Public Alerting System Common Look and Feel Guidance [Ref 32]. See Annex B, Configurable Parameters.
8. A WSP shall have two WSP Gateways designated for receipt of alerts from the NAADS WPA Gateway.
9. The WSP Gateway should incorporate redundancy and be designed to provide high reliability and availability that is equal to that of other critical telecommunication system components.
10. A Wireless Service Provider (WSP) may have redundant WSP Gateways in the WSP network to support distribution of WPA messages and to handle anticipated WPAM traffic levels. The WSP maintains the responsibility for the distribution of the alert message over the WSP's CBS.
11. Upon receipt of an alert message, the WSP Gateway shall respond back to the NAADS WPA Gateway with an acknowledgment that the alert message was received or an error indicating that the message was rejected.

6.1.3 WPA System Test Considerations

This Section defines the C-Interface requirements for WPA System Testing and C-Interface Link Testing.

6.1.3.1 WPA System Testing Considerations

1. The WPA System Test shall be initiated by the NAAD System Administrator or an Authorized Government Alerting Authority using a defined WPA Test Message that initiates a value of "Invisible Test" within in the XML Element known as "WPAC_deliveryChannel" in the WPAM.
2. The WSP's CBS shall process and deliver the WPAM containing the WPA Test Message immediately over their networks to the defined geo-targeted area using the WPA Test Channel (MI=4380).

   NOTE: WSP personnel may and are expected to generate their own internal test messages from their respective CBS using the WPA System Test Channel (MI-4380). However, because this activity occurs downstream of the WPA C-Interface, internal WSP testing is beyond the scope of this specification.

3. A WSP may forego a WPAS System Test if it is pre-empted by actual alert traffic or if an unforeseen condition in the CBS infrastructure precludes distribution of the WPAS System Test information. A WSP Gateway, upon receipt of a WPA System Test Message, shall immediately inform the NAADS WPA Gateway using an error response on the C-Interface that there is an unforeseen condition, which precludes distribution.

4. A WSP shall provide one or more mobile devices with the capability of receiving WPA System Test Messages.

6.1.3.2 Periodic C-Interface Testing (Link Test) Considerations

1. A WSP shall participate in periodic testing of the interface between the NAADS WPA Gateway and their WSP Gateway(s) using Link Test Messages. This periodic interface testing is not intended to test the WSP's infrastructure nor the mobile devices, but rather is used to validate the ongoing availability/viability of both gateways and the connectivity between said gateways.
2. This will result in the NAADS WPA Gateway generating a System Status of "System" and Message Type "Link Test" in the WPAM.
3. Each WSP Gateway shall send an acknowledgement to the NAADS WPA Gateway upon receipt of such an interface test message.
4. Actual alert Event Codes or Alert Messages or a WPA Delivery Channel value shall not be used for this periodic interface testing.
5. Link Test will be initiated on an automated schedule by the NAADS WPA Gateway as defined in Annex B, Configurable Parameters.

6.1.3.3 NAADS WPA Gateway Link Test Considerations

1. The NAADS WPA Gateway shall support the capability to initiate a WPA Link Test Messages on the C-Interface using a defined WPA Link Test message. Real Event Codes or Alert Messages or a WPA Delivery Channel shall not be used for the WPA System Test message.
2. The NAADS WPA Gateway shall support initiating Link Test Messages periodically over the C-Interface to verify the availability of the WSP Gateway. The frequency of the Link Testing is defined in Annex B, Configurable Parameters.
3. The NAADS WPA Gateway shall support the receipt and processing of WSP Gateway initiated interface test messages.

6.1.3.4 WSP Gateway Link Test Considerations

1. A WSP Gateway shall support the ability to receive a WPA Link Test Message initiated by the NAADS WPA Gateway and sent over the C-Interface.
2. A WSP shall be required to retain an automated log of WPA Link Test Messages received by the WSP Gateway from the NAADS WPA Gateway. Contents and retention period of this log shall be conformant with WSP archive policy, be consistent with standard industry practice and specific logging detail is beyond the scope of this specification.
3. The WSP Gateway shall be capable of receiving and responding to NAADS WPA Gateway initiated Link Test Messages which are periodically sent over the C-Interface to verify the availability of the WSP Gateway. The frequency of the Link Testing is defined in Annex B, Configurable Parameters.
4. As an option, the WSP Gateway may support Link Testing over the C-Interface to the NAADS WPA Gateway. This would be conducted on an as required basis by the WSP and is beyond the scope of this Specification.

6.1.4 C-Interface Overview

The complete set of message types exchanged between the NAADS WPA Gateway and the WSP Gateway is shown in the following figure. Note that all WPAC messages are exchanged using the XML-based [Ref 16] WPAC protocol (see Section 8.1.1, *WPAC Protocol*) over Hypertext Transfer Protocol (HTTP) (see Section 8.1.2, *HTTP*).

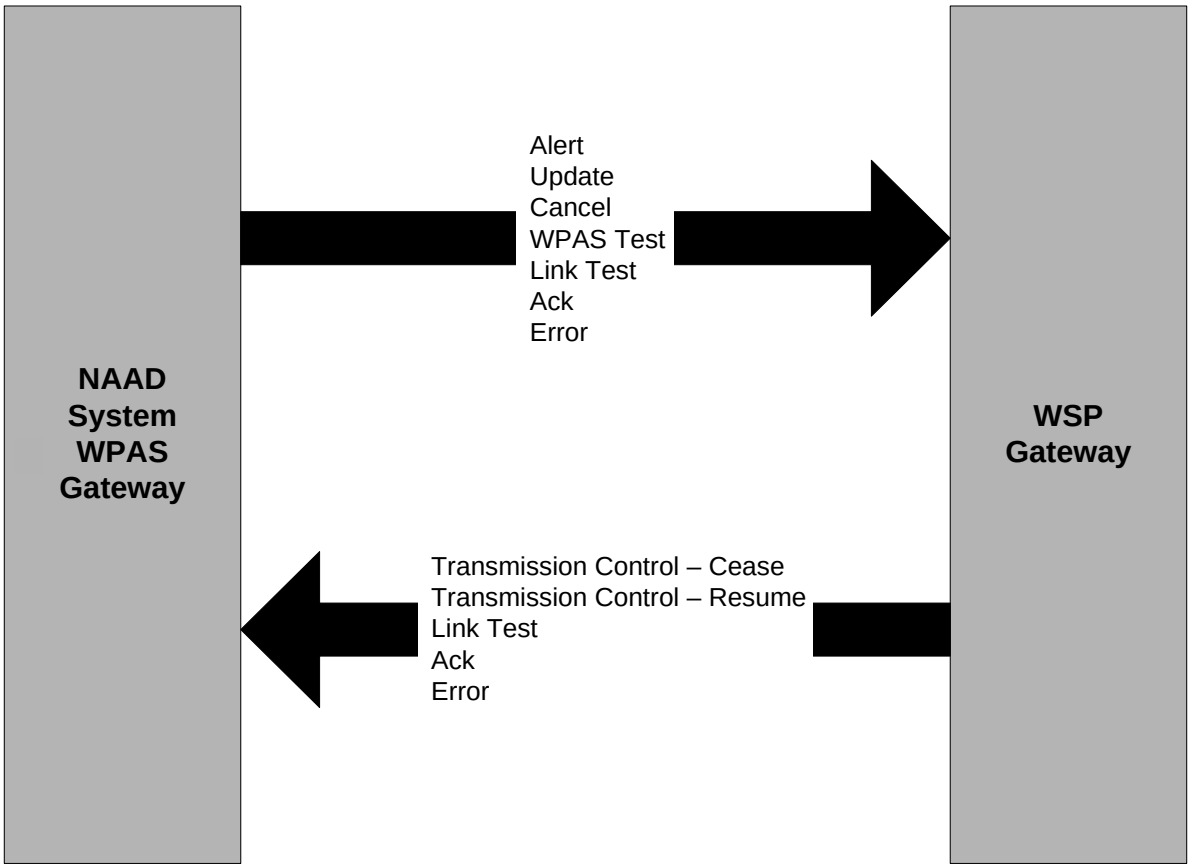

Figure 2: NAADS WPA Gateway to WSP Gateway Message Type Summary

The following table provides the characteristics of the WPAC messages from the NAADS WPA Gateway to the WSP Gateway:

Table 1: Characteristics of Messages issued by the NAADS WPA Gateway

MESSAGE TYPE	FORMAT	DESCRIPTION	TRANSMISSION FREQUENCY (PEAK)
Alert	WPAC	Included in the WPAM. Instructs the Cell Broadcast System to issue a new Alert Message.	Maximum number of Alert, Update, and/or Cancel Messages sent per minute is defined in Annex B, Configurable Parameters. Note: Some Alert or Update Messages expire before being cancelled.
Update	WPAC	Included in the WPAM. Instructs the Cell Broadcast System to cancel (see below) a previous Alert Message and to issue a new replacement Alert Message (see above).	
Cancel	WPAC	Included in the WPAM. Instructs the Cell Broadcast System to cancel (stop broadcasting) a previous Alert Message as defined by a specific identifier number.	
WPA System Test	WPAC	Included in the WPAM. Instructs the Cell Broadcast System to issue a new System Test Message over the WPA System Test (Invisible) Channel (MI=4380).	Frequency determined by CRTC Test Policy, SOREM Test Policy, the NAAD System and WSPs.
Link Test	WPAC	Included in the WPAM. Generated periodically by the NAADS WPA Gateway to validate the availability of the WSP Gateway.	The automated frequency of the Link Testing is defined in Annex B, Configurable Parameters.
Ack	WPAC	Issued by the NAADS WPA Gateway to the WSP Gateway to confirm successful receipt of a command (i.e. Transmission Control – Cease), acknowledge or error message from the WSP Gateway.	As Required.
Error	WPAC	Issued by the NAADS WPA Gateway to the WSP Gateway to confirm unsuccessful receipt of a command (i.e. Transmission Control – Cease), acknowledge or error message from the WSP Gateway.	As Required.

The following table provides the characteristics of the WPAC messages from the WSP Gateway to the NAADS WPA Gateway:

Table 2: Characteristics of Messages issued by the WSP Gateway

MESSAGE TYPE	FORMAT	DESCRIPTION	TRANSMISSION FREQUENCY (PEAK)
Transmission Control – Cease	WPAC	Sent by the WSP Gateway to instruct the NAADS WPA Gateway to discontinue transmission of messages to the WSP Gateway.	As Required. Should be used very infrequently during WSP Gateway maintenance, failures, or processing overload conditions.
Transmission Control – Resume	WPAC	Sent by the WSP Gateway to instruct the NAADS WPA Gateway to resume transmission of messages to the WSP Gateway.	As Required. Should be used very infrequently during WSP Gateway maintenance, failures, or processing overload conditions.
Link Test	WPAC	May be generated by the WSP Gateway to validate connectivity with and availability of NAADS WPA Gateway.	Used occasionally and as required by the WSP.

MESSAGE TYPE	FORMAT	DESCRIPTION	TRANSMISSION FREQUENCY (PEAK)
Ack	WPAC	Issued by the WSP Gateway to the NAADS WPA Gateway to confirm successful receipt of a WPAM from the NAADS WPA Gateway.	Proportionally reactive to the number of Alert, Update, Cancel Messages, WPA System Test Messages and Link Tests issued by the NAADS WPA Gateway.
Error	WPAC	Issued by the WSP Gateway to the NAADS WPA Gateway to confirm unsuccessful receipt of a WPAM from the NAADS WPA Gateway.	As Required.

6.2 NAADS WPA Gateway Requirements

In addition to the NAADS WPA Gateway requirements contained within this section and sub-sections, there are also additional NAADS WPA Gateway requirements in other sections of this Specification. For example, there are protocol requirements for the NAADS WPA Gateway contained in *Section 8.2.6.1, NAADS WPA Gateway Initiated Messages.*

6.2.1 NAADS WPA Gateway Requirements for WSP Profile

The NAADS WPA Gateway shall maintain a WSP Profile for each WSP Gateway Group (this includes tow or more WSP Gateways per WSP). The profile shall provide the information necessary for the NAADS WPA Gateway to communicate with each WSP Gateway. A Fully Qualified Domain Name or IP address shall be maintained for each WSP Gateway.

1. [WPA-C-RQMT-0100] The NAADS WPA Gateway message exchange shall be exclusive to WSP Gateways per the WSP profile for each WSP Gateway Group.
2. [WPA-C-RQMT-0110] The NAADS WPA Gateway shall maintain verifiable identities for approved WSP Gateways.
3. [WPA-C-RQMT-0120] The NAADS WPA Gateway shall maintain a WSP profile that includes the parameters identified in *Table 3: WSP Profile Definition*, *NAADS WPA Gateway Definition of WSP Profile*.

6.2.1.1 NAADS WPA Gateway Definition of WSP Profile

[WPA-C-RQMT-0200] The WSP Profile in the NAADS WPA Gateway shall contain the parameters defined in the following table:

Table 3: WSP Profile Definition

PARAMETER	DESCRIPTION	RANGE OF VALUES
WSP Name	Unique identification of WSP.	Text string
WSP Gateway A Address	IP address or Fully Qualified Domain Name. Uniquely identifies the WSP Gateway.	IP address / Text string
WSP Gateway B Address alternate	IP address or Fully Qualified Domain Name. Uniquely identifies the WSP Gateway.	IP address / Text string (optional)

NOTE: For information about port number assignments, see Section 8.1.2, *HTTP*.

6.2.2 NAADS WPA Gateway Requirements for IP Network Connectivity

IP Network Connectivity between the NAADS WPA Gateway and the WSP Gateway shall be secure, robust and introduce minimal latency to the end-to-end processing of Alert Messages and WPA System Test Messages. There are multiple established and standardized IP Network Connectivity Solutions that can facilitate these requirements. As such, the specific technology to be employed shall be determined by the NAAD System and each WSP and is beyond the scope of this specification.

6.2.3 NAADS WPA Gateway Requirements for Message Transmission

The NAADS WPA Gateway sends Alert Messages, Update Messages, Cancel Messages, WPA System Test Messages or Link Tests to the WSP Gateway. Alert, Update and Cancel Messages are triggered by the reception of a CAP-CP message at the NAADS WPA Gateway. If the CAP-CP message is validated as meeting the criteria for a Broadcast Immediate (BI) Alert and translated successfully into the WPAC format, WPAMs shall result. WPA System Test or Link Test Messages are originated in the NAADS WPA Gateway.

Link Test Messages are generated at the NAADS WPA Gateway to indicate to the WSP Gateway that the NAADS WPA Gateway and the interface are available. The WPA System Test Message is generated to test the end-to end service including the WSP Gateway and WSP Infrastructure as part of a WPA System Test.

The NAADS WPA Gateway also responds to WSP Gateway messages with either an Ack or an Error message. The format for each of the messages is detailed in *Section 8.5, WPAC Message Types & Example XML*.

For a redundant WSP Gateway configuration, the NAADS WPA Gateway sends all Alert, Update, Cancel, and WPA System Test Messages to both WSP Gateways in a WSP Gateway Group unless it has received a Transmission Control – Cease message from a specific WSP Gateway to discontinue transmission.

The NAADS WPA Gateway sends all Link Test Messages to all WSP Gateways that did not send a Transmission Control – Cease message to discontinue transmission.

1. [WPA-C-RQMT-0400] The NAADS WPA Gateway shall send the following message types to the WSP Gateway per the WPAC protocol:
   - *Alert (Section 8.5.1, Alert Message)*
   - *Update (Section 8.5.2, Update Message)*
   - *Cancel (Section 8.5.3, Cancel Message)*
   - *WPA System Test (Section 8.5.7, WPA System Test Message)*
   - *Link Test (Section 8.5.6, Link Test Message)*
   - *Ack (Section 8.5.4, Ack Message)*
   - *Error (Section 8.5.5, Error Message)*
2. [WPA-C-RQMT-0410] The NAADS WPA Gateway shall send an Alert message to the WSP Gateway Group when triggered by the reception of a CAP-CP Alert message that meets the criteria for a BI WPA Update Message.
3. [WPA-C-RQMT-0420] The NAADS WPA Gateway shall send an Update Message to the WSP Gateway Group when triggered by the reception of an upstream CAP-CP Update message that meets the criteria for a BI Update Message.

4. [WPA-C-RQMT-0430] The NAADS WPA Gateway shall send a Cancel message to the WSP Gateway Group when triggered by the reception of an upstream CAP-CP Cancel Message or CAP-CP Update Message that meets the criteria for a WPA Alert Cancellation.
5. [WPA-C-RQMT-0440] The NAADS WPA Gateway shall send a WPA System Test Message to the WSP Gateway Group in accordance with CRTC, SOREM, NAAD System and/or WSP Test Policy.
6. [WPA-C-RQMT-0450] The NAADS WPA Gateway shall send a Link Test Message in accordance with the Link Testing Period as defined in Annex B, Configurable Parameters to each WSP Gateway that did not send a Transmission Control – Cease message.
7. [WPA-C-RQMT-0460] The NAADS WPA Gateway shall send an Ack message to the WSP Gateway when a WSP Gateway message has been received without error.

   NOTE: See Section 8.7, *Error Handling*, for a description of the error checks.
8. [WPA-C-RQMT-0470] The NAADS WPA Gateway shall send an Error message to the WSP Gateway when a WSP Gateway message has been received with any error.

   NOTE: See Section 8.7, *Error Handling*, for a description of the error checks. Also see error codes in Table 31: *Definition of WPAC Response Codes*.
9. [WPA-C-RQMT-0480] The NAADS WPA Gateway shall send all Alert, Update, Cancel, and WPA System Test messages to all WSP Gateways unless it received a Transmission Control – Cease message from a specific WSP Gateway to discontinue transmission.

6.2.4 NAADS WPA Gateway Requirements for Message Reception

The NAADS WPA Gateway receives Transmission Control - Cease and Transmission Control - Resume messages from the WSP Gateway. It may also receive Link Test Messages from the WSP Gateway as a means for the WSP Gateway to check the availability of the interface and/or the NAADS WPA Gateway. The NAADS WPA Gateway also receives Ack and Error messages from the WSP Gateway in response to messages sent to the WSP Gateway. The format for each of these messages is detailed in *Section 8.5, WPAC Message Types & Example XML*.

1. [WPA-C-RQMT-0500] The NAADS WPA Gateway shall receive and process the following message types from the WSP Gateway per the WPAC protocol:
   - *Transmission Control - Cease (Section 8.5.8, Transmission Control – Cease Message)*
   - *Transmission Control - Resume (Section 8.5.9, Transmission Control – Resume Message)*
   - *Link Test (Section 8.5.6, Link Test Message)*
   - *Ack (Section 8.5.4, Ack Message)*
   - *Error (Section 8.5.5, Error Message)*
2. [WPA-C-RQMT-0510] The NAADS WPA Gateway shall receive and log each Transmission Control – Cease message from the WSP Gateway.
3. [WPA-C-RQMT-0520] The NAADS WPA Gateway shall receive and log each Transmission Control - Resume message from the WSP Gateway.
4. [WPA-C-RQMT-0530] The NAADS WPA Gateway shall receive and log Link Test Messages from the WSP Gateway.
5. [WPA-C-RQMT-0540] The NAADS WPA Gateway shall receive and log Ack messages from the WSP Gateway.
6. [WPA-C-RQMT-0550] The NAADS WPA Gateway shall receive and log Error messages from the WSP Gateway.

7. [WPA-C-RQMT-0560] The NAADS WPA Gateway shall respond to all messages from a WSP Gateway even if that WSP Gateway has sent a Transmission Control – Cease message.

6.3 WSP Gateway Requirements

In addition to the WSP Gateway requirements contained within this Section and sub-Sections, there are also additional WSP Gateway requirements in other Sections of this Specification. For example, there are protocol requirements for the WSP Gateway contained in *Section 8.2.6.2, WSP Gateway Initiated Messages*.

6.3.1 WSP Gateway Requirements for NAADS WPA Gateway Profile

The NAADS WPA Gateways shall send messages to all WSP Gateways. The IP addresses, or Fully Qualified Domain Names for each NAADS WPA Gateway shall be maintained in a NAADS WPA Gateway profile within each WSP Gateway. A WSP Gateway may receive messages from any of the NAADS WPA Gateways in the profile. No more than 2 NAADS WPA Gateways are active at any given time per WSP Gateway Group.

1. [WPA-C-RQMT-0700] WSP Gateway message exchanges with the NAADS WPA Gateways shall be exclusivee to those defined in the NAADS WPA Gateway profile.
2. [WPA-C-RQMT-0710] The WSP Gateway shall accept and process messages received from any of the NAADS WPA Gateways identified in the NAADS WPA Gateway profile.
3. [WPA-C-RQMT-0720] The WSP Gateway shall maintain verifiable identities for approved NAADS WPA Gateways.

6.3.1.1 WSP Gateway Definition of NAADS WPA Gateway Profile

[WPA-C-RQMT-0600] The WSP Gateway shall maintain a NAADS WPA Gateway profile that includes the parameters identified in the following table:

Table 4: NAADS WPA Gateway Profile Definition

PARAMETER	DESCRIPTION	RANGE OF VALUES
NAADS WPA Gateway Address (n)	IP address or Fully Qualified Domain Name (See Note 1). Uniquely identifies both Geo-Redundant NAADS WPA Gateways.	IP address / Text string

NOTE 1: When a Domain Name uniquely identifies the NAADS WPA Gateway, the IP address of the NAADS WPA Gateway may be provisioned in the WSP's network (i.e., at the option of the WSP) for Domain Name Service implemented in the WSP's network.

NOTE 2: For information about port number assignments, see *Section 8.1.2, HTTP*.

6.3.2 WSP Gateway Requirements for IP Network Connectivity

IP Network Connectivity between the WSP Gateway and the NAADS WPA Gateway shall be secure, robust and introduce minimal latency to the end-to-end processing of Alert Messages and WPA System Test Messages. There are multiple established and standardized IP Network Connectivity Solutions that can facilitate these requirements. As such, the specific technology to be employed shall be determined by the NAAD System and each WSP and is beyond the scope of this specification.

6.3.3 WSP Gateway Requirements for Message Transmission

Individual WSP Gateways in the WSP Gateway Group shall send a Transmission Control – Cease message to the NAADS WPA Gateways to discontinue transmission of all messages (e.g., for a planned or unplanned outage) and a Transmission Control – Resume to the NAADS WPA Gateways to resume transmission of all messages. Although the Geo-Redundant NAADS WPA Gateways operate in an Active-Active Failover configuration, transmission from each NAADS WPA Gateways is controlled independently.

The WSP Gateway may also send Link Test Messages to each NAADS WPA Gateway to check the availability of the interface and the availability of the individual NAADS WPA Gateway itself. The WSP Gateway may send a Link Test Message to any NAADS WPA Gateway in its NAADS WPA Gateway Profile but shall never allow more than two IP connections (one for each NAADS WPA Gateway) at any given time. The WSP Gateway also sends Ack and Error messages to the NAADS WPA Gateway in response to WPAMs received from a NAADS WPA Gateway. An acknowledgement response from WSP Gateway to the NAADS WPA Gateway indicates that the WPAM has been correctly received, validated and processed over the Cell Broadcast System (CBS). The format for each of these messages is detailed in *Section 8.5, WPAC Message Types & Example XML*.

1. [WPA-C-RQMT-0900] The WSP Gateway shall send the following message types to the NAADS WPA Gateway per the WPAC protocol:
   - *Transmission Control - Cease (Section 8.5.8, Transmission Control – Cease Message)*
   - *Transmission Control - Resume (Section 8.5.9, Transmission Control – Resume Message)*
   - *Link Test (Section 8.5.6, Link Test Message)*
   - *Ack (Section 8.5.4, Ack Message)*
   - *Error (Section 8.5.5, Error Message)*
2. [WPA-C-RQMT-0910] The WSP Gateway shall send an Error message to a NAADS WPA Gateway when a message has been received from that NAADS WPA Gateway with an error.

   NOTE: See *Section 8.7, Error Handling*, for a description of the error checks. Also see error codes in Table 32: *Definition of WPAC Response Codes*.

3. [WPA-C-RQMT-0920] The WSP Gateway shall send a Transmission Control – Cease message to the NAADS WPA Gateways in its NAADS WPA Gateway profile to discontinue the transmission of messages from that NAADS WPA Gateway.

4. [WPA-C-RQMT-0930] The WSP Gateway shall send a Transmission Control – Resume message to the NAADS WPA Gateways in its NAADS WPA Gateway profile to resume the transmission of messages from that NAADS WPA Gateway.

   NOTE: It is valid to send a Transmission Control – Resume message when there was no previous Transmission Control – Cease message sent.

5. [WPA-C-RQMT-0940] The WSP Gateway shall send a Link Test Message to the NAADS WPA Gateway to determine the status of communication with the NAADS WPA Gateway.

   NOTE: The initiation of a Link Test is optional for the WSP Gateway.

6. [WPA-C-RQMT-0950] The WSP Gateway shall send an Ack message to a NAADS WPA Gateway when a message has been received from that NAADS WPA Gateway without error.

   NOTE: See *Section 8.7, Error Handling*, for a description of the error checks.

6.3.4 WSP Gateway Requirements for Message Reception

The WSP Gateway receives Alert, Update, or Cancel Message, WPA System Test or Link Test from the NAADS WPA Gateway. The WPA System Test Message is received from the NAADS WPA Gateway by the WSP Gateway to test the WSP Infrastructure. The WSP Gateway receives Link Test Messages from the NAADS WPA Gateway to indicate to the WSP Gateway that the NAADS WPA Gateway and the interface are available. The WSP Gateway also responds to NAADS WPA Gateway messages with either an Ack or an Error message. The format for each of the messages is detailed in *Section 8.5, WPAC Message Types & Example XML*.

1. [WPA-C-RQMT-1000] The WSP Gateway shall receive and process the following message types from the NAADS WPA Gateway in the WPAC protocol:
   - *Alert (Section 8.5.1, Alert Message)*
   - *Update (Section 8.5.2, Update Message)*
   - *Cancel (Section 8.5.3, Cancel Message)*
   - *WPA System Test (Section 8.5.7, WPA System Test Message)*
   - *Link Test (Section 8.5.6, Link Test Message)*
   - *Ack (Section 8.5.4, Ack Message)*
   - *Error (Section 8.5.5, Error Message)*
2. [WPA-C-RQMT-1010] The WSP Gateway shall receive and log Alert messages from the NAADS WPA Gateway.

   NOTE: The WSP Gateway shall attempt to distribute the WPA alert through its infrastructure. This function is beyond the scope of this Specification.
3. [WPA-C-RQMT-1020] The WSP Gateway shall receive and log Update messages from the NAADS WPA Gateway.

   NOTE: The WSP Gateway shall stop broadcasting an identified Alert Message and shall attempt to broadcast the Update through its infrastructure. This function is beyond the scope of this Specification.
4. [WPA-C-RQMT-1030] The WSP Gateway shall receive and log Cancel messages from the NAADS WPA Gateway.

   NOTE: The WSP Gateway shall attempt to stop broadcasting the identified Alert Message. This function is beyond the scope of this Specification.
5. [WPA-C-RQMT-1040] If the WSP Gateway receives an "Update" message and cannot make an association with a previously issued Alert Message, the WSP Gateway shall process the Update as a new Alert Message.
6. [WPA-C-RQMT-1041] If the WSP Gateway receives a Cancel message and cannot make an association with a previously issued Alert Message, the WSP Gateway shall respond to the WPA Cancel message with a WPAC Error message (see *Table 32: Definition of WPAC Response Codes*).
7. [WPA-C-RQMT-1050] The WSP Gateway shall receive and log WPA System Test messages from the NAADS WPA Gateway.
8. [WPA-C-RQMT-1060] The WSP Gateway shall receive and log Link Test Messages from the NAADS WPA Gateway.
9. [WPA-C-RQMT-1070] The WSP Gateway shall receive and log Ack messages from the NAADS WPA Gateway.
10. [WPA-C-RQMT-1080] The WSP Gateway shall receive and log Error messages from the NAADS WPA Gateway.

11. [WPA-C-RQMT-1110] If conditions at the WSP Gateway preclude distribution of the WPA System Test information, the WSP Gateway shall respond to the WPA System Test message with an Error message (see Table 32: Definition of WPAC Response Codes).

6.4 Quality of Service Requirements

6.4.1 Prioritization

All WPA Alerts, Updates Cancel Messages and System Test Messages have the same priority.

1. [WPA-C-RQMT-1200] The NAADS WPA Gateway shall send all alerts to the WSP Gateway on a First In - First Out (FIFO) basis.

6.4.2 Message Queuing

The NAADS WPA Gateway shall queue valid outgoing WPAMs to a WSP Gateway if it cannot send the message to any WSP Gateway in the WSP Gateway Group immediately. The NAADS WPA Gateway shall remove from the queue all messages, which are no longer valid for, broadcast (i.e., cancelled, updated, expired).

The following requirements apply to the entire group of NAADS WPA Gateways interacting with a WSP Gateway:

1. [WPA-C-RQMT-1300] The NAADS WPA Gateway shall queue outgoing WPAMs to a WSP Gateway Group as long as the message is still valid for broadcast in accordance with Annex B, Configurable Parameters, it cannot send the message to any WSP Gateway in the WSP Gateway Group and has not received an Ack/Error response.
2. [WPA-C-RQMT-1310] The NAADS WPA Gateway shall remove messages from the queue which are no longer valid for broadcast (i.e., cancelled, updated, expired).
3. [WPA-C-RQMT-1320] The NAADS WPA Gateway shall send all queued messages in FIFO order to a WSP Gateway when an IP connection is established with that WSP Gateway.

6.4.3 Redundancy

To mitigate the risk of equipment, operating system, application or communication failures, both the NAAD System WPA Gateways and WSP Gateways shall be implemented in an Active-Active Redundant configuration. Aside from hardware or software failures, Redundancy will also mitigate the unlikely situation where the NAAD System WPA Gateways may be issuing an Alert, Update or Cancel Message while a WSP Gateway is simultaneously issuing a Transmission Control-Cease Message. Should this situation occur, the NAAD System WPA Gateways shall be able to forward the Alert, Update or Cancel Message to the alternate WSP Gateway.

1. [WPA-C-RQMT-1400] The NAADS WPA Gateways and WSP Gateways shall be implemented in an Active-Active Redundant configuration.

7 C-INTERFACE CALL FLOWS

This section contains the call flows for the transactions that can occur across the C-Interface. These call flows are grouped as follows:

- *WPAC alert message call flows;*
- *Link test message call flows;*
- *WPA System Test call flow;*
- *Transmission Control call flows.*

Note that the call flows may describe general operations within the NAADS WPA Gateway and WSP Gateway but specific details of these operations are beyond the scope of this Specification.

7.1 WPAC Alert Message Call Flows

From the point of view of the C-Interface, the WPAC Alert, Update, and Cancel Message types have the same call flow. The variances in the call flows result from WPAC alert message transmission control and from invalid messages across the C-Interface. Consequently, this Section provides the following call flows, which are applicable to WPA Alert, Update, and Cancel Message types:

- *WPAC alert message.*
- *Invalid WPAC alert message call flow.*

7.1.1 WPAM Call Flow

The WPAC alert, update, and cancel message types have the same call flow across the C-Interface. The following figure with its descriptions of the associated call flow steps defines the call flow for WPAC Alert, Update, and Cancel message types:

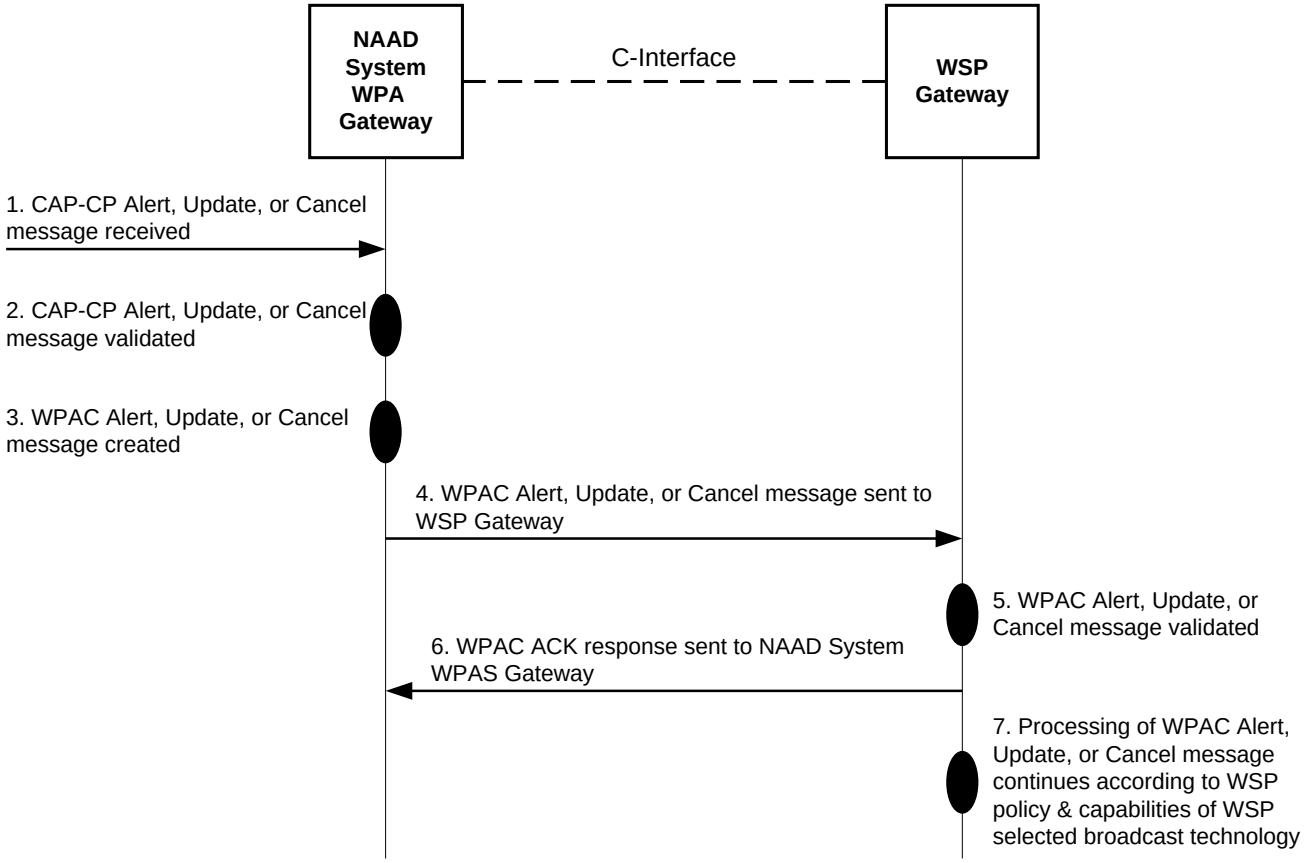

Figure 3: WPAC Message Call Flow

1. A CAP-CP Alert, Update, or Cancel message is received by the NAADS WPA Gateway. This function is beyond the scope of this Specification.
2. The received CAP-CP Alert, Update, or Cancel message is validated by the NAADS WPA Gateway (i.e., meets the criteria for a Wireless BI alert). The original CAP-CP message is stored on the NAAD System for potential archival and retrieval at https://alerts.pelmorex.com/filearchiveaccess/. The upstream behavior of the NAADS WPA Gateway is beyond the scope of this Specification.
3. The NAADS WPA Gateway constructs a WPAC Alert, Update, or Cancel message using attributes from the received CAP-CP message. The conversion process used within the NAADS WPA Gateway is beyond the scope of this Specification.
4. The NAADS WPA Gateway sends the WPAC Alert, Update, or Cancel message to the WSP Gateway via the C-Interface.
5. The WSP Gateway attempts to validate the received WPAM and the received WPAM passes validation.
6. The WSP Gateway sends a WPAC Acknowledgement (ACK) message back to the NAADS WPA Gateway via the C-Interface.
7. The processing of the received WPAC Alert, Update, or Cancel message continues according to WSP policy and according to the capabilities of the CBS over the Mandatory Public Channel (MI=4370).

7.1.2 Invalid WPAM Call Flow

All WPAC alert messages received by WSP Gateway over the C-Interface are validated for content, format, and structure. The following figure with its descriptions of the associated call flow steps define the call flow for an invalid WPAC Alert, Update, or Cancel messages received by the WSP Gateway over the C-Interface:

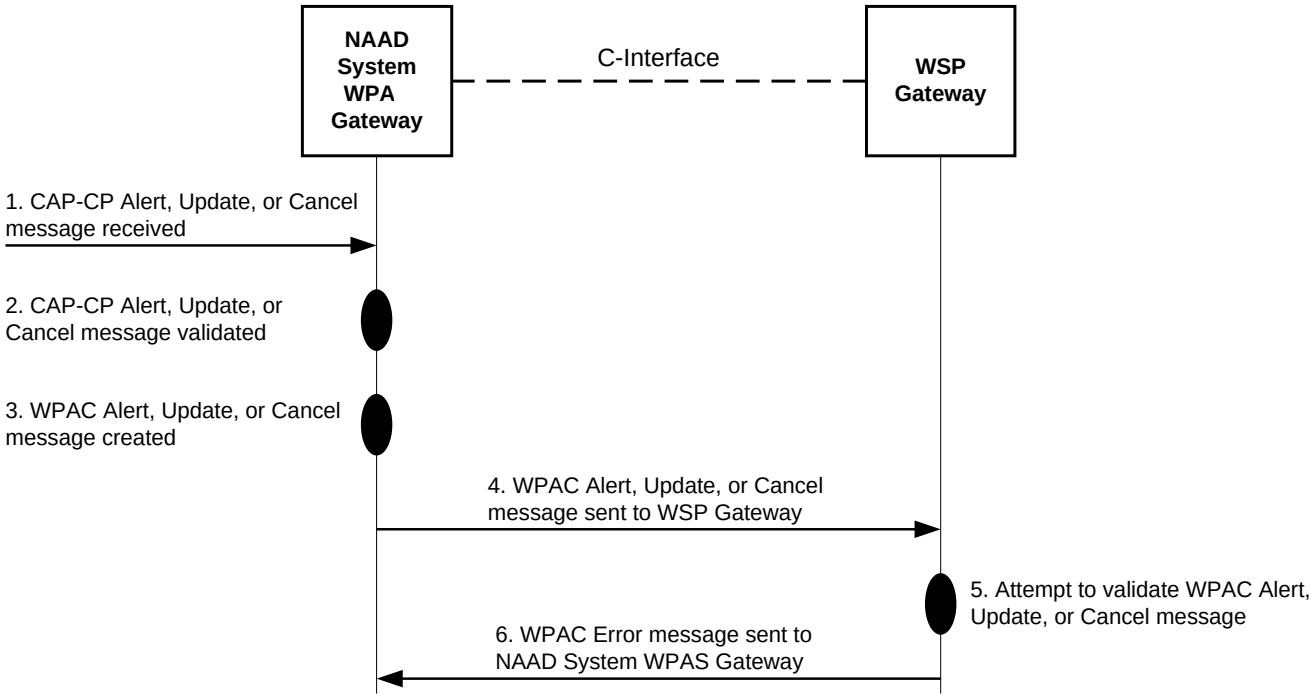

Figure 4: Invalid WPAC Message Call Flow

1. An upstream CAP-CP Alert, Update, or Cancel message is received by the NAADS WPA Gateway. This function is beyond the scope of this Specification.
2. The received CAP-CP Alert, Update, or Cancel message is validated by the NAADS WPA Gateway. The received CAP-CP message is stored on the NAAD System and made available through on their public website https://alerts.pelmorex.com/filearchiveaccess/ for potential review and/or retrieval by the WSP. The upstream behavior of the NAADS WPA Gateway is beyond the scope of this Specification.
3. The NAADS WPA Gateway constructs a WPAC Alert, Update, or Cancel message using attributes from the originating CAP-CP message. The conversion process used within the NAADS WPA Gateway is beyond the scope of this Specification.
4. The NAADS WPA Gateway sends the WPAC Alert, Update, or Cancel message to the WSP Gateway via the C-Interface.
5. The WSP Gateway attempts to validate the received WPAM and the received WPAM fails validation.
6. The WSP Gateway sends a WPAC Error message with the validation failure reason back to the NAADS WPA Gateway via the C-Interface.

   NOTE: The behavior of the NAADS WPA Gateway when a WPAC Error message with the validation failure reason is received from the WSP Gateway is beyond the scope of this Specification.
7. The WSP Gateway returns to and idle state to await delivery of the next WPAM or Link Test.

7.2 Link Test Message Call Flows

One of the WPA requirements is to verify the availability of the C-Interface and the availability of the WPA functionality. The Link Test Message between the NAADS WPA Gateway and the WSP Gateway is used to comply with this requirement. This Section provides the following link test call flows:

- *Link Test Message to WSP Gateway call flow.*
- *Invalid Link Test Message to WSP Gateway call flow.*
- *Link Test Message from WSP Gateway call flow.*
- *Invalid Link Test Message from WSP Gateway call flow.*

7.2.1 Link Test Message to WSP Gateway Call Flow

The NAADS WPA Gateway shall periodically (see Annex B, Configurable Parameters) issue Link Test Messages to the WSP Gateway to verify the availability of the C-Interface and the WSP Gateway. The following figure with its descriptions of the associated call flow steps define the call flow for a Link Test Message sent from the NAADS WPA Gateway to the WSP Gateway over the C-Interface:

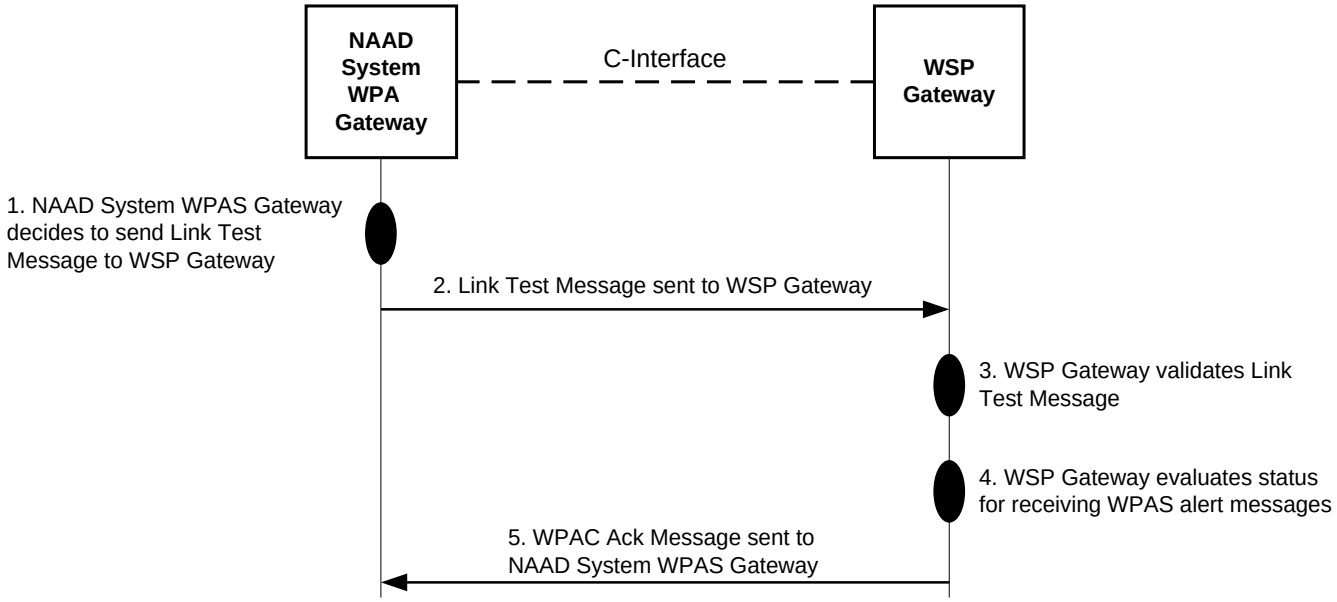

Figure 5: Link Test Message to WSP Gateway Call Flow

1. The NAADS WPA Gateway decides to send a link test to the WSP Gateway and constructs the Link Test Message. The methodology for the creation of the Link Test Messages by the NAADS WPA Gateway is beyond the scope of this Specification.
2. The NAADS WPA Gateway sends the Link Test Message to the WSP Gateway via the C-Interface.
3. The WSP Gateway validates the received Link Test Message and the received Link Test Message passes validation.
4. The WSP Gateway determines its ability to receive WPA alert messages. This determination is beyond the scope of this Specification.

5. The WSP Gateway sends a WPAC Ack Message back to the NAADS WPA Gateway.

7.2.2 Invalid Link Test Message to WSP Gateway Call Flow

Link Test Messages received by WSP Gateway over the C-Interface are validated for content, format, and structure. The following figure with its descriptions of the associated call flow steps define the call flow for invalid Link Test Message sent to the WSP Gateway over the C-Interface:

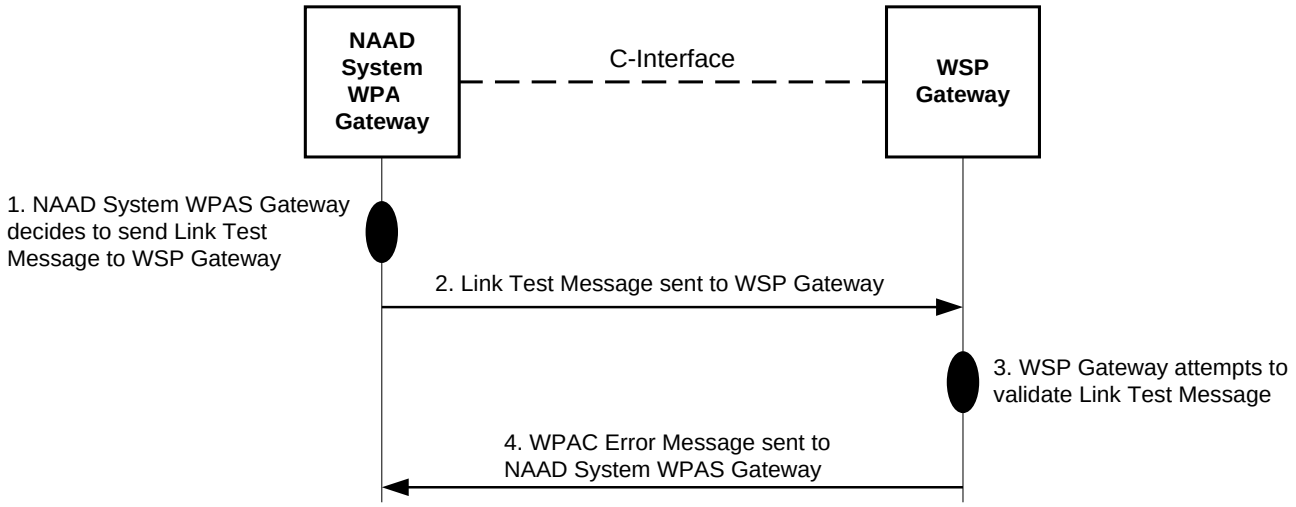

Figure 6: Invalid Link Test Message from NAADS WPA Gateway Call Flow

1. The NAADS WPA Gateway decides to send a link test to the WSP Gateway and constructs the Link Test Message. The methodology for the creation of the Link Test Messages by the NAADS WPA Gateway is beyond the scope of this Specification.
2. The NAADS WPA Gateway sends the Link Test Message to the WSP Gateway via the C-Interface.
3. The WSP Gateway attempts to validate the received Link Test Message and the received Link Test Message fails validation.
4. The WSP Gateway sends a WPAC Error message with the validation failure reason back to the NAADS WPA Gateway via the C-Interface.

   NOTE: The behavior of the NAADS WPA Gateway when a WPAC Error message with the validation failure reason is received from the WSP Gateway is beyond the scope of this Specification.

7.2.3 Link Test Message from WSP Gateway Call Flow (Optional)

As a WSP implementation option, the WSP Gateway shall be able to send a Link Test Message to the NAADS WPA Gateway to verify the availability of the C-Interface and the WPA functionality. The following figure with its descriptions of the associated call flow steps define the call flow for a Link Test Message sent from the WSP Gateway to the NAADS WPA Gateway over the C-Interface:

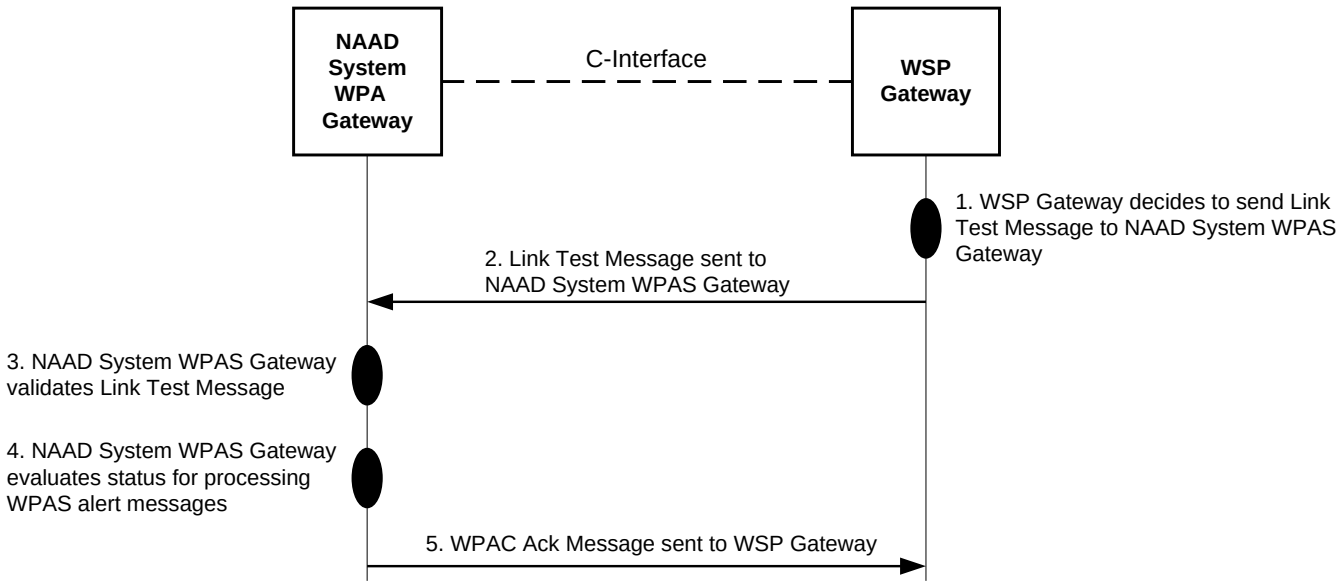

Figure 7: Link Test Message from WSP Gateway Call Flow

1. The WSP Gateway decides to send a link test to the NAADS WPA Gateway and constructs the Link Test Message. The methodology and frequency for the creation of the Link Test Messages from the WSP Gateway is beyond the scope of this Specification.
2. The WSP Gateway sends the Link Test Message to the NAADS WPA Gateway via the C-Interface.
3. The NAADS WPA Gateway validates the received Link Test Message and the received Link Test Message passes validation.
4. The NAADS WPA Gateway determines the availability of the WPA functionality. The methodologies to determine the availability of the WPA functionality are subject to the policies of the WSP Gateway Administrator and are beyond the scope of this Specification.
5. The NAADS WPA Gateway sends a WPAC Ack Message back to the WSP Gateway.

7.2.4 Invalid Link Test Message from WSP Gateway Call Flow

Link Test Messages received by NAADS WPA Gateway over the C-Interface are validated for content, format, and structure. The following figure with its descriptions of the associated call flow steps define the call flow for invalid Link Test Message sent to the NAADS WPA Gateway over the C-Interface:

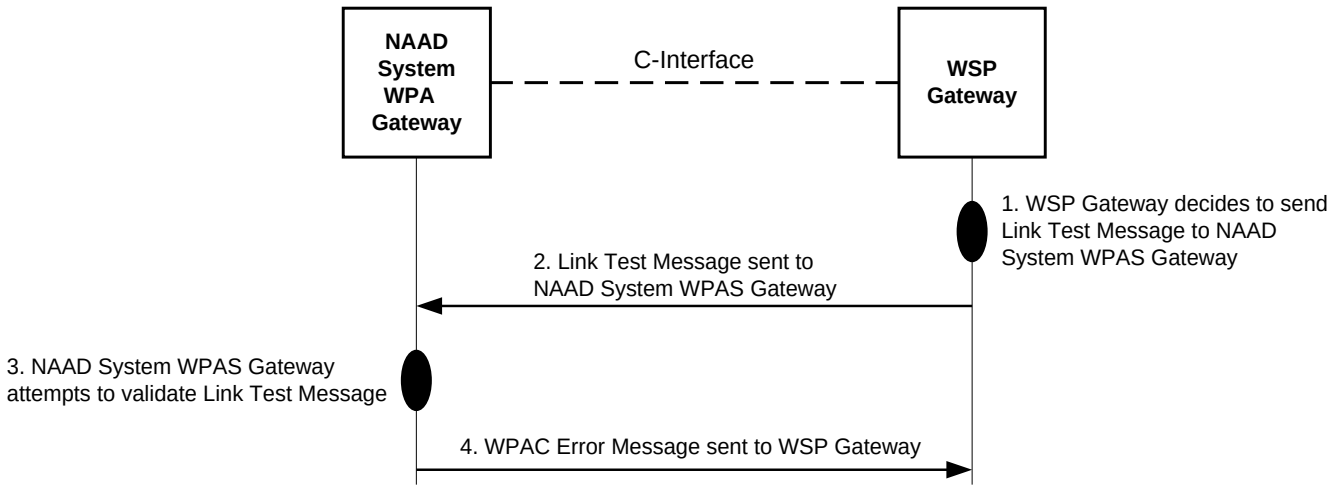

Figure 8: Invalid Link Test Message from WSP Gateway Call Flow

1. The WSP Gateway decides to send a link test to the NAADS WPA Gateway and constructs the Link Test Message. The methodology and frequency for the creation of the Link Test Messages from the WSP Gateway is beyond the scope of this Specification.
2. The WSP Gateway sends the Link Test Message to the NAADS WPA Gateway via the C-Interface.
3. The NAADS WPA Gateway attempts to validate the received Link Test Message and the received Link Test Message fails validation.
4. The NAADS WPA Gateway sends a WPAC Error message with the validation failure reason back to the WSP Gateway via the C-Interface.

   NOTE: Any additional behavior by the NAADS WPA Gateway when a WPAC Error message with the validation failure reason is sent to the WSP Gateway is beyond the scope of this Specification.

7.3 WPA System Test Call Flow

The NAADS WPA Gateway may issue a WPA System Test Message to the WSP Gateway. The following figure with its descriptions of the associated call flow steps define the call flow for a WPA System Test Message sent from the NAADS WPA Gateway to the WSP Gateway over the C-Interface:

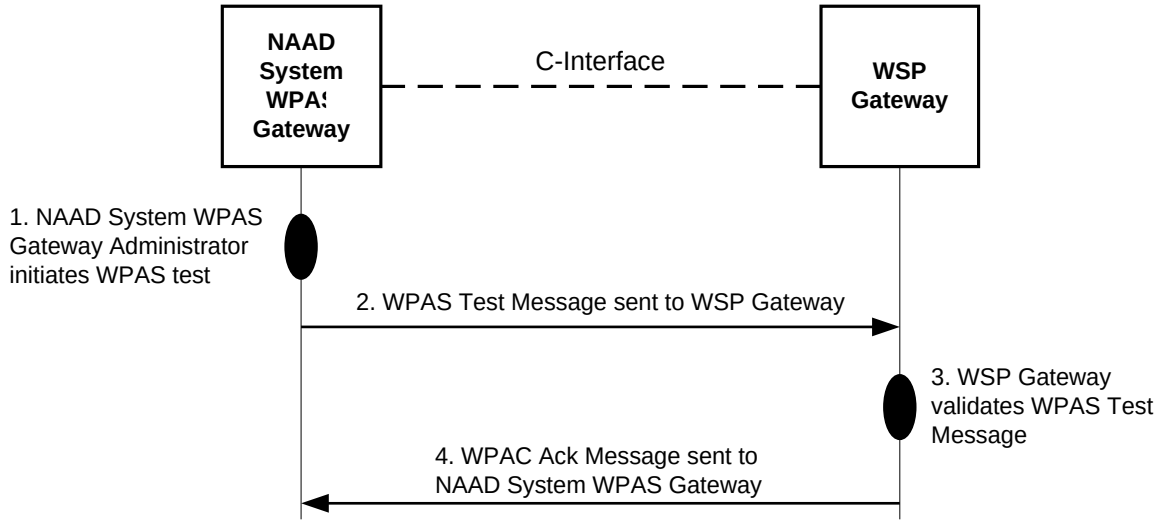

Figure 9: WPA System Test Call Flow

1. An Alerting Authority or authorized NAAD System Administrator initiates a WPA System Test in the NAAD System. The operational details associated with this function is beyond the scope of this Specification.
2. The NAADS WPA Gateway sends the WPA System Test Message to the WSP Gateway via the C-Interface.
3. The WSP Gateway validates the received WPA System Test Message and the received WPA System Test Message passes validation.
4. The WSP Gateway sends a WPAC Ack Message back to the NAADS WPA Gateway via the C-Interface.
5. The WSP Gateway (as part of the CBS) processes the WPA System Test Message over the Invisible WPA Test Channel (MI=4380)

   NOTE: Upon receipt of the WPA System Test Message, if the WSP determines an unforeseen condition in the WSP infrastructure that precludes distribution of the WPA System Test information, the WSP Gateway sends an Error message back to the NAADS WPA Gateway indicating that an unforeseen condition in WSP infrastructure precludes distribution of the WPA System Test information. The WSP determination of types of unforeseen conditions and procedures for precluding WPA System Test processing are beyond the scope of this Specification.

7.4 Transmission Control Message Call Flows

The WSP Gateway may request message traffic on C-Interface destined for the WSP Gateway be ceased or resumed via maintenance commands on the WSP Gateway or internal error processing. This Section provides the following transmission control call flows:

- *Cease transmissions call flow*
- *Resume transmissions call flow*

7.4.1 Cease Transmissions Call Flow

The WSP Gateway may request transmissions of all messages destined for the WSP Gateway be ceased via maintenance command on the WSP Gateway or internal error processing.

The following figure with its descriptions of the associated call flow steps defines the call flow for a Transmission Control - Cease Message sent from the WSP Gateway to the NAADS WPA Gateway over the C-Interface:

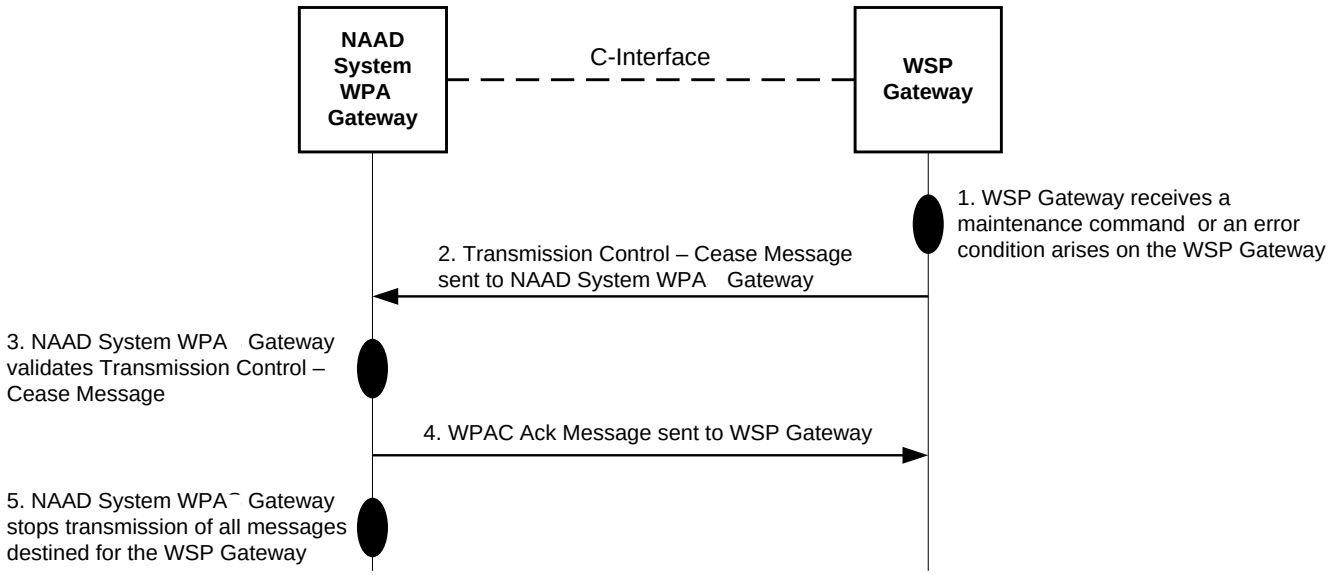

Figure 10: Cease Transmissions Call Flow

1. The WSP Gateway receives a maintenance command to request the NAADS WPA Gateway stop transmissions of all messages destined for that WSP Gateway or an error condition arises which prevents the WSP Gateway from processing any further messages from the NAADS WPA Gateway.
2. The WSP Gateway sends the Transmission Control - Cease Message to the NAADS WPA Gateway via the C-Interface.
3. The NAADS WPA Gateway validates the Transmission Control – Cease Message received from the WSP Alert Gateway.
4. The NAADS WPA Gateway sends a WPAC Ack Message back to the WSP Gateway. If the WSP Gateway is malfunctioning or offline due to scheduled or unscheduled maintenance, it may choose to ignore the Transmission Control Acknowledgement Message. If the WSP Gateway is online, the WPAC Ack/Error Message shall be captured in the WSP log files.
5. The NAADS WPA Gateway stops transmissions of all messages destined for that WSP Gateway.

7.4.2 Resume Transmissions Call Flow

Once the maintenance or error condition that triggered the stop of message transmission over the C-Interface is cleared, the WSP Gateway informs the NAADS WPA Gateway that transmission of messages may resume. The following figure with its descriptions of the associated call flow steps defines the call flow for a Transmission Control – Resume Message sent from the WSP Gateway to the NAADS WPA Gateway over the C-Interface:

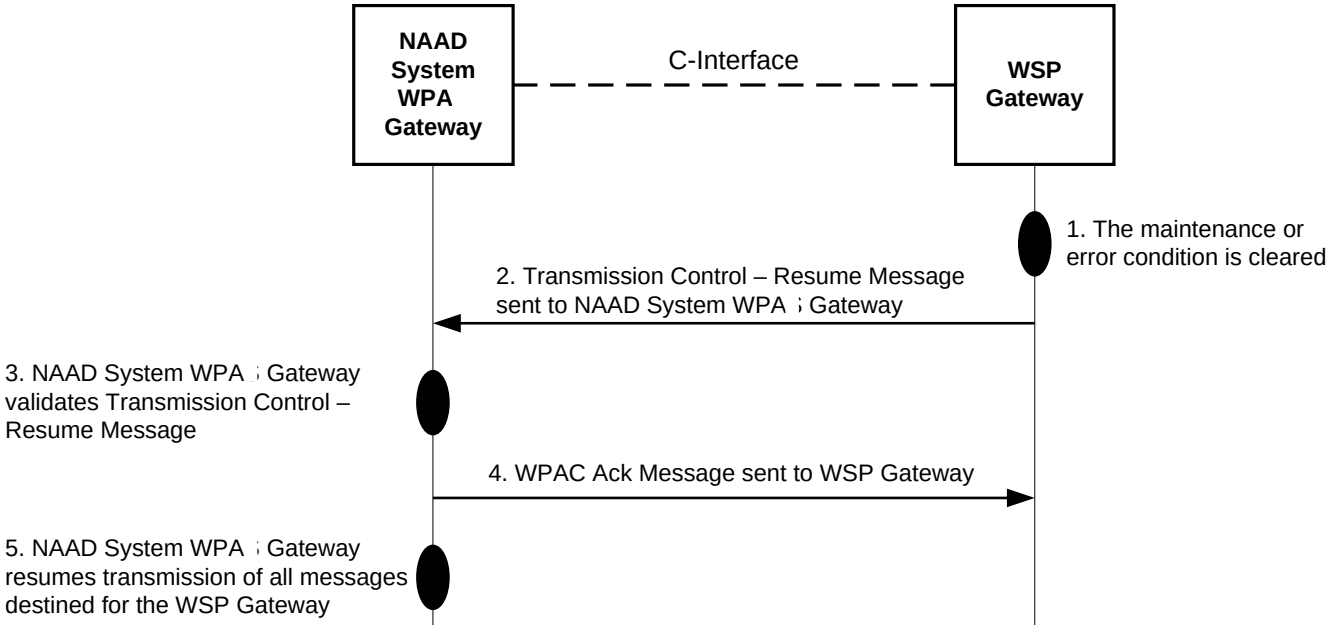

Figure 11: Resume Transmissions Call Flow

1. The maintenance or error condition that triggered the stop of message transmission over the C-Interface is cleared.
2. The WSP Gateway sends the Transmission Control – Resume Message to the NAADS WPA Gateway via the C-Interface.
3. The NAADS WPA Gateway validates the received Transmission Control – Resume Message from the WSP Alert Gateway.
4. The NAADS WPA Gateway sends a WPAC Ack Message back to the WSP Gateway.
5. The NAADS WPA Gateway may resume transmission of messages destined for the WSP Gateway.

8 NAADS WPA GATEWAY TO WSP GATEWAY COMMUNICATION PROTOCOL REQUIREMENTS AND DEFINITION

The Wireless Public Alerting C-Interface protocol supports delivery and acknowledgement of a new, updated, or cancelled Wireless Public Alert Message (WPAM) between the NAADS WPA Gateway and the WSP Gateway. The protocol also enables testing, verification of network entity availability, and transmission control.

This description of the protocol between the NAADS WPA Gateway and the WSP Gateway is structured as follows:

- *Application layer*
- *Message structure*
- *Element definition*
- *XML definition*
- *Transport protocol*
- *C-Interface Security*

8.1 Application Layer

8.1.1 WPAC Protocol

The majority of the messages exchanged between the NAADS WPA Gateway and the WSP Gateway (see Table 1: *Characteristics of Messages issued by the NAADS WPA Gateway,* Table 2: *Characteristics of Messages issued by the WSP Gateway and* Table 5: *WPAC XML Elements, Values and Function*) shall be in the WPAC format. The WPAC protocol content by message type is captured in *Section 8.5, WPAC Message Types & Example XML* while the details of the WPAC Protocol are captured in *Section 8.2, Message Structure,* and *8.3, Element Definition*.

The following *Table 5: WPAC XML Elements, Values and Function* provides a general overview of how the various XML Elements and related Value options within the WPAC affects the functionality of the CBS. Some XML Elements and Values (WPAC_attributes) direct specific CBS functionality while others (WPAC_info and WPAC_area) provides the message content and geo-targeting information respectively. In many cases, the XML Elements and related Values merely provide contextual information for archive purposes only.

Table 5: WPAC XML Elements, Values and Function

WPAC ELEMENT NAME	WPAC ELEMENT VALUE	FUNCTION
	WPAC_attributes	The following elements are WPAC Attributes that may be required to construct a Wireless Public Alert Message (WPAM)
WPAC_version	1.0 (Example)	Instructs the Cell Broadcast System (CBS) as to which version of the Wireless Public Alerting Service Architecture for C-Interface (WPAC) is being employed. Maintained in CBS Archive for each Message processed or rejected.
WPAC_gatewayID	205.136.9.70 (Example)	Identifies the NAADS WPA Gateway to the WSP Gateway by way of a unique IP address or Fully Qualified Domain Name (URL). Maintained in CBS Archive for each Message processed or rejected.
WPAC_identifier	60000001 (Example)	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_referencedIdentifier	60000000 (Example)	Identifies Alert, Update or Cancel Message with a unique reference identifier to facilitate subsequent Update and Cancel Messages. Maintained in CBS Archive for each Message processed or rejected.
WPAC_referencedIdentifier CAPCP	urn:oid:2.49.0.1.124.2499364842.2017 (Example)	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_deliveryChannel	Mandatory Public	Instructs the CBS that the Message being issued is an Alert, Update or Cancel Message that shall be processed on the Mandatory Public Channel (MI=4370). Maintained in CBS Archive for each Message processed or rejected.
	Invisible Test	Instructs the CBS that the Message being issued is a Test Message for Technical or Administrative Purposes and that it is to be processed on the Invisible Test Channel (MI=4380). Maintained in CBS Archive for each Message processed or rejected.
WPAC_sender	cap-pac@canada.ca (example)	Identifies the sending Authorized Government Alerting Authority for archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_sent	2017-06-17T18:57:37.9991869Z (example)	Identifies the Sent Time for the Alert, Update, Cancel or WPA System Test Message. Maintained in CBS Archive for each Message processed or rejected.
WPAC_status	Actual	Instructs the CBS that the Message being issued is an actual Alert, Update or Cancel Message.
	System	Instructs the CBS that the Message being issued is a Test Message for Technical or Administrative Purposes.
WPAC_msgType	Alert	Instructs the CBS that the Message being issued is an Alert Message. Maintained in CBS Archive for each Message processed or rejected.
	Update	Instructs the CBS that a previous Alert Message or Update Message as identified by the unique reference identifier must be cancelled (broadcasting discontinued) and that a new replacement Alert Message must be processed. Maintained in CBS Archive for each Message processed or rejected.

WPAC ELEMENT NAME	WPAC ELEMENT VALUE	FUNCTION
	Cancel	Instructs the CBS that a previous Alert Message or Update Message as identified by the unique reference identifier must be cancelled (broadcasting discontinued). Maintained in CBS Archive for each Message processed or rejected.
	Ack	Acknowledges successful receipt, validation and processing of information by the NAADS WPA Gateway or WSP Gateway from the other gateway. Maintained in CBS Archive for each Message processed or rejected.
	Error	Advises of an Error in receipt, validation and/or processing of information by the NAADS WPA Gateway or WSP Gateway from the other gateway. Maintained in CBS Archive for each Message processed or rejected.
	WPAS Test	Instructs the CBS that the Message being issued is WPAS System Test Message. Maintained in CBS Archive for each Message processed or rejected.
	Link Test	Issued regularly by the NAAD System WPA Gateway and as required by the WSP Gateway to validate the connectivity with and availability of the other gateway. Maintained in CBS Archive for each Message processed or rejected.
	Transmission Control - Cease	Instructs the NAADS WPA Gateway that a specific WSP Gateway is unable to process an Alert, Update, Cancel or WPA System Test Message. Maintained in CBS Archive for each Message processed or rejected.
	Transmission Control - Resume	Instructs the NAADS WPA Gateway that a specific WSP Gateway can resume processing an Alert, Update, Cancel or WPA System Test Message. Maintained in CBS Archive for each Message processed or rejected.
WPAC_responseCode	100	Supports Error Message to provide further detail to the NAADS WPA Gateway as follows - Initiate CBS functionality - invalid-naad-system-wpas-alert-gateway-id. Maintained in CBS Archive for each Message rejected.
	101	Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows - Initiate CBS functionality - protocol–version-not-supported. Maintained in CBS Archive for each Message processed or rejected.
	102	Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows - Initiate CBS functionality - server-error. Maintained in CBS Archive for each Message processed or rejected.
	103	Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows - Initiate CBS functionality - invalid-format. Maintained in CBS Archive for each Message processed or rejected.

WPAC ELEMENT NAME	WPAC ELEMENT VALUE	FUNCTION
	104	Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows - Initiate CBS functionality - invalid-element XXX. Maintained in CBS Archive for each Message processed or rejected.
	105	Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows - Initiate CBS functionality - missing-element XXX. Maintained in CBS Archive for each Message processed or rejected.
	106	Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows - Initiate CBS functionality - operation-not-allowed. Maintained in CBS Archive for each Message processed or rejected.
	107	Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows - Initiate CBS functionality - operation-pre-empted. Maintained in CBS Archive for each Message processed or rejected.
	108	Supports Error Message to provide further detail to the NAADS WPA Gateway from the WSP Gateway as follows - Initiate CBS functionality - wpas-test-distribution-precluded. Maintained in CBS Archive for each Message processed or rejected.
WPAC_note	For <WPAC_responseCode> = 100: invalid-naad-system-wpas-alert-gateway-id	Note for NAADS WPA Gateway Administrator stating that Sending gateway identifier is not valid. Maintained in CBS Archive for each Message processed or rejected.
	For <WPAC_responseCode> = 101: protocol-version-not-supported	Note for NAADS WPA Gateway Administrator stating that Gateway does not support the indicated protocol version. Maintained in CBS Archive for each Message processed or rejected.
	For <WPAC_responseCode> = 102: server-error	Note for NAADS WPA Gateway Administrator stating that General error in the server. Maintained in CBS Archive for each Message processed or rejected.
	For <WPAC_responseCode> = 103: invalid-format	Note for NAADS WPA Gateway Administrator stating that Received XML has an invalid format. Maintained in CBS Archive for each Message processed or rejected.
	For <WPAC_responseCode> = 104: invalid-element XXX	Note for NAADS WPA Gateway Administrator stating that XXX replaced with name of invalid element. Maintained in CBS Archive for each Message processed or rejected.
	For <WPAC_responseCode> = 105: missing-element XXX	Note for NAADS WPA Gateway Administrator stating that XXX replaced with name of missing element. Maintained in CBS Archive for each Message processed or rejected.

WPAC ELEMENT NAME	WPAC ELEMENT VALUE	FUNCTION
	For <WPAC_responseCode> = 106: operation-not-allowed	Note for NAADS WPA Gateway Administrator stating that Requested operation is not allowed. Maintained in CBS Archive for each Message processed or rejected.
	For <WPAC_responseCode> = 107: operation-pre-empted	Note for NAADS WPA Gateway Administrator stating that Requested operation was pre-empted and not completed. Maintained in CBS Archive for each Message processed or rejected.
	For <WPAC_responseCode> = 108: wpas-test-distribution-precluded	Note for NAADS WPA Gateway Administrator stating that Unforeseen condition precluding distribution of WPAS Test information. Maintained in CBS Archive for each Message processed or rejected.
WPAC_CAPCPIdentifier	urn:oid:2.49.0.1.124.2499364842.2017 (example)	Documents original CAPCP Identifier. For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_CAPCPSent	2017-09-11T19:40:13-00:00 (example)	Documents original CAPCP Sent Time. For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
	WPAC_info	The following elements are WPAC Information Values that may be required to construct a Wireless Public Alert Message (WPAM)
WPAC_category	Value copied from CAP-CP <category> Example: Met	Documents Event Category. For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_eventCode	Value copied from CAP-CP <eventCode> Example: tornado	Documents Event Description . For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_responseType	Value copied from CAP-CP <responseType> Example: Shelter & Place	Documents Event Call to Action. For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_severity	Value copied from CAP-CP <severity> Example: Extreme	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_urgency	Value copied from CAP-CP <urgency> Example: Immediate	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_certainty	Value copied from CAP-CP <certainty> Example: Observed	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_expires	2017-09-11T19:40:13-00:00 (Example)	Instructs the CBS to terminate the Alert Update or WPA System Test Message at the specified time. Must be present or the WPAM may be rejected. Maintained in CBS Archive for each Message processed or rejected.
WPAC_senderName	Example: Environment Canada	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_language	English	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
	French	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.

WPAC ELEMENT NAME	WPAC ELEMENT VALUE	FUNCTION
	English and French	For archival reference only. Maintained in CBS Archive for each Message processed or rejected. The "English and French" value should be used by the NAADS Alert Gateway for any language in a WPAM to ensure appropriate processing in CBS.
WPAC_descriptionLength	578 (Example)	Instructs the CBS as to the number of Characters and Spaces in the Text Field of the Alert, Update or WPA System Test Message. For archival reference only. Character length must conform to the Minimum and Maximum Character Length as defined in Annex B, Configurable Parameters or the WPAM may be rejected. Maintained in CBS Archive for each Message processed or rejected.
WPAC_description	This is a test /// Ceci est un test (Example)	Provides the CBS with the actual English, French, Bilingual English + French or Bilingual French + English Text Information that must be forwarded to subscribers screens. Maintained in CBS Archive for each Message processed or rejected. Maintained in CBS Archive for each Message processed or rejected.
	WPAC_area	The following elements are WPAC Area Values that are required to geo-target the delivery of a Wireless Public Alert Message (WPAM). Maintained in CBS Archive for each Message processed or rejected.
WPAC_areaDesc	City of Toronto (Example)	For archival reference only. Maintained in CBS Archive for each Message processed or rejected. Maintained in CBS Archive for each Message processed or rejected.
WPAC_polygon	Value copied from CAP-CP <polygon> 43.2035,-81.2241 43.2034,-81.224 (Example)	Provides the CBS with the actual Longitude and Latitude information necessary to geo-target the alert to the cellular coverage area that intersects with the Emergency Alert Area. Maintained in CBS Archive for each Message processed or rejected.
WPAC_circle	Value copied from CAP-CP <circle>	Provides the CBS with the actual Longitude and Latitude information necessary to geo-target the alert to the cellular coverage area that intersects with the Emergency Alert Area. Maintained in CBS Archive for each Message processed or rejected.
WPAC_geocode	3539033 (Example)	For archival reference only. Maintained in CBS Archive for each Message processed or rejected.
WPAC_signature	X56re34568jdudu8 (Example)	For archival reference and subsequent validation only. Maintained in CBS Archive for each Message processed or rejected.

Note that for each WPAC message, Conditional and Optional elements defined in the protocol are to be included as applicable to the particular message.

1. [WPA-C-RQMT-2510] Each Alert message shall contain the mandatory message elements and associated values provided in the following tables:
   - *Table 13: Elements of Alert Attributes Segment for Alert Message*
   - *Table 14: Elements of Alert Info Segment for Alert Message*

- *Table 15: Elements of Alert Area Segment for Alert Message*
- *Table 16: Elements of Alert Signature Segment for Alert Message*

2. [WPA-C-RQMT-2520] Each Update message shall contain the mandatory message elements and associated values provided in the following tables:
   - *Table 17: Elements of Alert Attributes Segment for Update Message*
   - *Table 18: Elements of Alert Info Segment for Update Message*
   - *Table 19: Elements of Alert Area Segment for Update Message*
   - *Table 20: Elements of Alert Signature Segment for Update Message*
3. [WPA-C-RQMT-2540] The WPAC_area shall contain at least one instance of WPAC_circle or WPAC_polygon elements and/or WPAC-geocode for all Alert Messages.

   NOTE: The WPAC_area may contain multiple <WPAC_geocode> <elements and may additionally contain one or more instances of <WPAC_polygon>, or <WPAC_circle>.
4. [WPA-C-RQMT-2550] The number of paired values of points (i.e., latitude/longitude pairs) used to define the polygon in the WPAC_polygon element shall be limited to a maximum of 150.
5. [WPA-C-RQMT-2560] Each Cancel message shall contain the mandatory message elements and associated values provided in the following table:
   - *Table 21: Elements of Alert Attributes Segment for Cancel Message*
6. [WPA-C-RQMT-2570] Each WPA System Test message shall contain the mandatory message elements and associated values provided in the following tables:
   - *Table 26: Elements of Alert Attributes Segment for WPA System Test Message*
   - *Table 27: Elements of Alert Info Segment for WPA System Test Message*
   - *Table 28: Elements of Alert Area Segment for WPA System Test Message*
   - *Table 29: Elements of Alert Signature Segment for WPA System Test Message*
7. [WPA-C-RQMT-2580] Each Link Test Message shall contain the mandatory message elements and associated values provided in the following table:
   - *Table 25: Elements of Alert Attributes Segment for Link Test Message*
8. [WPA-C-RQMT-2590] Each Ack message shall contain the mandatory message elements and associated values provided in the following table:
   - *Table 23: Elements of Alert Attributes Segment for Ack Message*
9. [WPA-C-RQMT-2600] Each Error message shall contain the mandatory message elements and associated values provided in the following table:
   - *Table 24: Elements of Alert Attributes Segment for Error Message*
10. [WPA-C-RQMT-2610] Each Transmission Control – Cease message shall contain the mandatory message elements and associated values provided in:
    - *Table 30: Elements of Alert Attributes Segment for Transmission Control – Cease Message.*
11. [WPA-C-RQMT-2620] Each Transmission Control – Resume message shall contain the mandatory message elements and associated values provided in:
    - *Table 31: Elements of Alert Attributes Segment for Transmission Control – Resume Message.*
12. [WPA-C-RQMT-2630] All WPAC messages shall adhere to the XML schema in *Section 8.4 WPAC Message XML Definition.*
13. [WPA-C-RQMT-2640] The value of the WPAC_identifier shall be increased monotonically for each and every message issued by the sending gateway.

14. [WPA-C-RQMT-2650] The WPAC_version element shall be set to "1.0" for this version of the Specification.

8.1.2 HTTP

HTTP [Ref 1] shall be the application level protocol used by the NAADS WPA Gateway and the WSP Gateway to exchange WPAC messages. The HTTP is a request/response protocol. The HTTP methods shall be limited to POST. The HTTP POST method shall be used by the NAADS WPA Gateway to send all messages in the WPAC protocol to the WSP Gateways, except Ack and Error messages. Similarly, the WSP Gateway shall use the HTTP POST method to send all messages in the WPAC protocol to the NAADS WPA Gateways except Ack and Error messages. Ack and Error messages shall be sent in the WPAC protocol XML in HTTP responses to the HTTP POSTs. HTTP 200 OK is used for all WPAC level responses (Ack and Error). HTTP error messages are only used to report HTTP-level errors. WPAC level error codes identify the particular errors. To summarize:

- An HTTP error shall indicate only an error at HTTP level;
- An HTTP 200 OK shall indicate HTTP has successfully received the message and delivered the XML body to WPAC protocol, but does not say anything about WPAC level processing; and
- WPAC errors are identified in WPAC_responseCode element, not from HTTP response codes.

Since there is no specific server resource associated with a WPAC message, the HTTP POST method shall use "*" as the Request_URI.

8.2 Message Structure

Each WPA C-Interface protocol message consists of a <WPAC_attributes> segment, which may contain a <WPAC_info> segment. The <WPAC_info> segment may contain one or more <WPAC_area> segments. (See *Figure 12: C-Interface Document Object Model* in *Section 8.2.5, WPAC Alert Message Document Object Model*.)

8.2.1 WPAC_attributes Segment

The WPAC_attributes segment provides basic information about the current message: its purpose, its source and its status, as well as unique identifier for the current message and a link to any other, related message. A <WPAC_attributes> segment may be used alone for message acknowledgements, cancels, or other system functions, but most <WPAC_attributes> segments shall include one <WPAC_info> segment.

8.2.2 WPAC_info Segment

The <WPAC_info> segment describes the information for the alert. This information includes the text field with the actual alert message, severity, and certainty and provides the text for the alert message.

8.2.3 WPAC_area Segment

The <WPAC_area> segment describes a geographic area to which the <WPAC_info> segment in which it appears applies.

8.2.4 WPAC_signature (Conditional)

The <WPAC_signature> provides a digital signature to indicate that the WPAM message was sent from the NAADS WPA Gateway.

8.2.5 WPAC Alert Message Document Object Model

The following figure shows the WPAC Alert Message document object model:

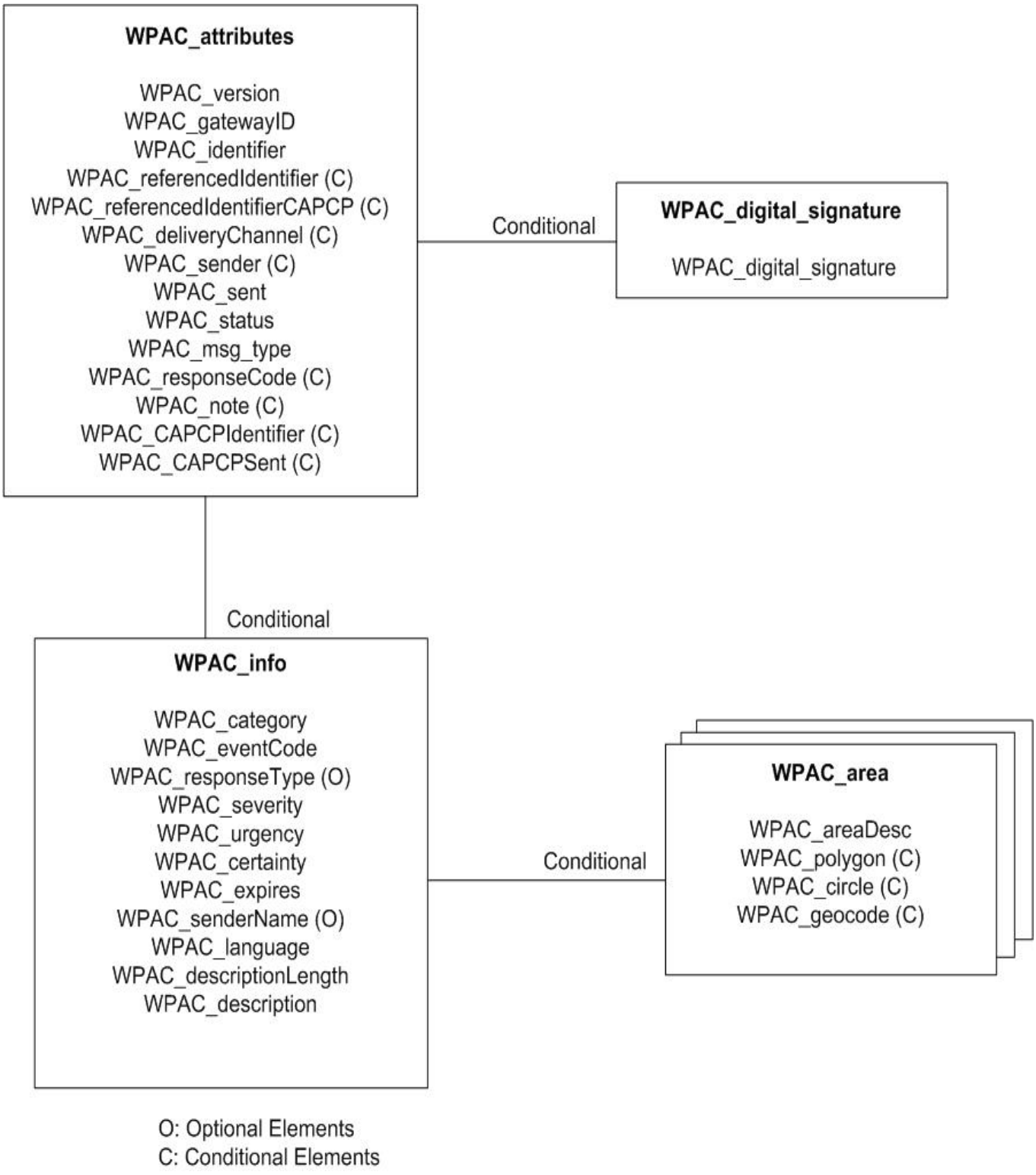

Figure 12: C-Interface Document Object Model

8.2.6 WPAC Message Types

The WPAC messages transmitted between the NAADS WPA Gateway and the WSP Gateway over the C-Interface can contain various segments. The following table defines the segments for each type of WPAM:

Table 6: WPAC Message Segments

WPAC MESSAGE	WPAC MESSAGE SEGMENTS
WPAC Alert Message	one <WPAC_attributes> segment one <WPAC_info> segment one or more <WPAC_area> segments
WPAC Update Message	one <WPAC_attributes> segment one <WPAC_info> segments one or more <WPAC_area> segments
WPAC Cancel Message	one <WPAC_attributes> segment
WPAC Link Test Message	one <WPAC_attributes> segment
WPAC WPAS Test Message	one <WPAC_attributes> segment one <WPAC_info> segment one or more <WPAC_area> segments
WPAC Transmission Control - Cease Message	one <WPAC_attributes> segment
WPAC Transmission Control - Resume Message	one <WPAC_attributes> segment
WPAC Ack Message	one <WPAC_attributes> segment
WPAC Error Message	one <WPAC_attributes> segment

The WPAC protocol requires a response to each message, with the exception of Ack and Error messages. *Table 7: NAADS WPA Gateway Initiated Messages* in Section 8.2.6.1, *NAADS WPA Gateway Initiated Messages,* and *Table 8: WSP Gateway Initiated Messages* in *Section 8.2.6.2, WSP Gateway Initiated Messages,* define the responses that are appropriate for messages initiated by the NAADS WPA Gateway and by the WSP Gateway, respectively. The Notes column in each table summarizes the meaning of the response.

8.2.6.1 NAADS WPA Gateway Initiated Messages

The following table summarizes the message types that may be initiated by the NAADS WPA Gateway and the expected responses from the WSP Gateway.

Table 7: NAADS WPA Gateway Initiated Messages

WPAC Message Type	Expected WSP Gateway Responses	Notes
Alert	Ack Error	An "Ack" indicates the WSP Gateway has successfully received the message and shall attempt to distribute the alert information. An "Error" indicates a problem with the message was identified by the WSP Gateway and no further processing shall be performed.
Update	Ack Error	An "Ack" indicates the WSP Gateway has successfully received the message and shall attempt to distribute the updated alert information. An "Error" indicates a problem with the message was identified by the WSP Gateway and no further processing shall be performed.
Cancel	Ack Error	An "Ack" indicates the WSP Gateway has successfully received the message and shall attempt to cancel distribution of the updated alert information. An "Error" indicates a problem with the message was identified by the WSP Gateway and no further processing shall be performed.
Link Test	Ack Error	An "Ack" indicates the WSP Gateway has successfully received the Link Test message and was able to respond. An "Error" indicates that the Link Test message was received by the WSP Gateway, but a problem was identified.
WPAS Test	Ack Error	An "Ack" indicates the WSP Gateway has successfully received the message and shall attempt to distribute the WPA System Test. An "Error" indicates a problem with the message was identified by the WSP Gateway and no further processing shall be performed.

1. [WPA-C-RQMT-2800] If the NAADS WPA Gateway receives an invalid or malformed acknowledgement or error response message from the WSP Gateway, the NAADS WPA Gateway should log this condition and shall not reply to the WSP Gateway with an error response.
2. [WPA-C-RQMT-2810] The WSP Gateway shall respond to each message from the NAADS WPA Gateway with one of the expected WSP Gateway responses valid for that particular message type per *Table 7: NAADS WPA Gateway Initiated Messages*.
3. [WPA-C-RQMT-2820] The WSP Gateway shall not send a message in response to an Ack or Error message from the NAADS WPA Gateway.
4. [WPA-C-RQMT-2830] If the NAADS WPA Gateway does not receive an expected response message (Ack or Error) from the WSP Gateway within the Message Response Time, the NAADS WPA Gateway shall retransmit the message in accordance with Annex B, Configurable Parameters.
5. [WPA-C-RQMT-2840] The NAADS WPA Gateway shall declare a WSP Gateway failure condition and generate a system notification if a message is retransmitted multiple times in accordance with Annex B, Configurable Parameters and a response is not received.

   NOTE: The NAADS WPA Gateway Administrator shall be notified in the event of a WSP Gateway failure and the NAADS WPA Gateway Administrator shall then also notify the appropriate Alerting Authorities about said failure. The details of these notification procedures are beyond the scope of this specification.

8.2.6.2 WSP Gateway Initiated Messages

The following table summarizes the message types that may be initiated by the WSP Gateway and the expected responses from the NAADS WPA Gateway.

Table 8: WSP Gateway Initiated Messages

WPAC MESSAGE TYPE	EXPECTED NAADS WPA GATEWAY RESPONSES	NOTES
Link Test	Ack Error	An "Ack" indicates the NAADS WPA Gateway has successfully received the Link Test message and was able to respond. An "Error" indicates that the Link Test message was received by the NAADS WPA Gateway, but a problem was identified.
Transmission Control - Cease	Ack Error	An "Ack" indicates the NAADS WPA Gateway has successfully received the Transmission Control – Cease Message and shall cease transmission of WPA alert messages to the WSP Gateway. An "Error" indicates that the Transmission Control – Cease Message was received by the NAADS WPA Gateway, but a problem was identified.
Transmission Control - Resume	Ack Error	An "Ack" indicates the NAADS WPA Gateway has successfully received the Transmission Control – Resume Message and shall resume transmission of WPA alert messages to the WSP Gateway. An "Error" indicates that the Transmission Control – Resume Message was received by the NAADS WPA Gateway, but a problem was identified.

1. [WPA-C-RQMT-2900] If the WSP Gateway receives an invalid or malformed acknowledgement or error response message from the NAADS WPA Gateway, the WSP Gateway should log this condition and shall not reply to the NAADS WPA Gateway with an error response.
2. [WPA-C-RQMT-2910] The NAADS WPA Gateway shall respond to each message from the WSP Gateway with one of the expected NAADS WPA Gateway responses valid for that particular message type per *Table 8: WSP Gateway Initiated Messages*.
3. [WPA-C-RQMT-2920] The NAADS WPA Gateway shall not send a message in response to an Ack or Error message from the WSP Gateway. The purpose of this requirement is to establish the demarcation at which ongoing and reciprocal Ack or Error messaging between the NAADS WPA Gateway and WSP Gateway will be discontinued.
4. [WPA-C-RQMT-2930] The WSP Gateway shall declare a NAADS WPA Gateway failure condition and generate a system notification if a message is retransmitted multiple times in accordance with Annex B, Configurable Parameters. System notification messages shall be sent to the WSP Gateway Administrator for further action with appropriate personnel such as the NAADS WPA Gateway Adminstration. The details of these operational procedures are beyond the scope of this specification.

8.3 Element Definition

This Section defines the elements for each segment of the WPAC message. These element definitions are grouped as follows:

- *Element definitions for the WPAC_attributes segment*
- *Element definitions for the WPAC_info segment*
- *Element definitions for the WPAC_area segment*
- *Definition of the WPAC_geocode element*

The definitions of Mandatory, Optional, and Conditional used in the element definition tables within this Section are as follows:

Mandatory (M)	This element is required.
Conditional (C)	This element may be required in the segment depending on the contents of other elements. The entry in the WPAC Definition column for this conditional element defines the conditions and values for this conditional element.
Optional (O)	This element may/may not be included in the segment. It is not required to process WPAMs over the WPAC. However, these elements may provide additional context and archival reference should the processing of the Alert Message be reviewed at a later time.

8.3.1 WPAC_attributes Segment Element Definition

The following table contains the definition of the elements of the WPAC_attributes segment. The WPAC_attributes segment is required in all WPAMs processed across the WPAC.

Table 9: WPAC_attributes Segment Element Definition

WPAC Element	Mandatory/ Optional/ Conditional	WPAC Definition
WPAC_attributes	M	(1) Surrounds WPAC attributes segment sub-elements. (2) Shall include the xmlns attribute referencing the WPAC URN [Ref 6] as the namespace, e.g.: <wpac:WPAC_attributes xmlns:wpac="wpac:1.0"> [sub-elements] </wpac:WPAC_attributes> (3) In addition to the specified sub-elements, may contain a <WPAC_info> block.
WPAC_Version	M	The version of the WPAC protocol. Used by the WSP Gateway and the NAADS WPA Gateway to identify the protocol version of the WPAC protocol.
WPAC_gatewayID	M	URI [Ref 2] or IP address of the NAADS WPA Gateway or the WSP Gateway sending the WPAC message.
WPAC_identifier	M	A numerical value to identify the message. When assigned by the NAADS WPA Gateway for Alert, Update, and Cancel Messages, the value is associated with the message identified by the CAP-CP identifier element. The NAADS WPA Gateway is responsible for mapping the CAP-CP identifier element to the WPAC_identifier element. When assigned by the NAADS WPA Gateway for other WPAC messages, the value is specified by the NAADS WPA Gateway. For messages initiated by the WSP Gateway, the value is assigned by the WSP Gateway.

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	WPAC DEFINITION
WPAC_referencedIdentifier	C	Required for an Update, Cancel, Ack, and Error WPAC message types. A numerical value identifying a referenced WPAC message, assigned by the NAADS WPA Gateway or WSP Gateway. When initiated by the NAADS WPA Gateway, this element may be associated with the message identified in the CAP-CP referenced element. The NAADS WPA Gateway is responsible for mapping the CAP-CP referenced element to the WPAC_referencedIdentifier element.
WPAC_deliveryChannel	C	Required to instruct the CBS that the Message being issued is an Alert or Update Message that shall be processed on the Mandatory Public Channel (MI=4370) or on the Invisible Test Channel (MI=4380). A value for this element is not required for a Cancel, Ack, Error or Link Test Message.
WPAC_referencedIdentifierCAPCP	C	Required for an Update and Cancel WPAC message types. Specifies the CAP-CP identifier of the message corresponding to the referenced WPAM.
WPAC_sender	C	Required for Alert, Update, and Cancel WPAC message types. Identifies the originator of this alert. May be used by the WSP for logging purposes only. NAADS WPA Gateway uses the CAP-CP sender element to populate this element.
WPAC_sent	M	The date and time the message is sent by the gateway in Date and Time.
WPAC_status	M	This element is used to identify actual alert messages from messages used for internal system use only. NAADS WPA Gateway may use the CAP-CP status element to populate this element. Code Values: "**Actual**" - Actionable by all targeted recipients "**System**" - For messages that support alert network internal functions (Link Test, Transmission Control – Cease, Transmission Control - Resume, WPA SYSTEM TEST, Ack and Error).

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	WPAC DEFINITION
WPAC_msgType	M	This element identifies the message type. For an Alert, Update, or Cancel message, the NAADS WPA Gateway may use the CAP-CP msgType element to populate this element. This element is also used to identify response messages and link test messages. Code Values: "**Alert**" - Initial information requiring attention by targeted recipients. "**Update**" - Updates and supersedes the earlier message(s) identified in <WPAC_referencedIdentifier>. "**Cancel**" - Cancels the earlier message(s) identified in <WPAC_referencedIdentifier>. "**Ack**" - Acknowledges receipt and acceptance of the message(s) identified in <WPAC_referencedIdentifier>. "**Error**" indicates rejection of the message(s) identified in <WPAC_referencedIdentifier>; explanation should appear in <WPAC_note>. "**WPAS Test**" indicates a WPA System Test message. "**Link Test**" indicates a "link test" message sent by the NAADS WPA Gateway or the WSP Gateway to verify the availability of the other Gateway. "**Transmission Control - Cease**" indicates the far end is to cease transmission (see Section 7.5.8, *Transmission Control – Cease Message*). "**Transmission Control – Resume**" indicates the far end may resume transmissions (see Section 7.5.9, *Transmission Control – Resume Message*).
WPAC_responseCode	C	Required for Error WPAC message type. This element contains the WPA Response Codes (see Section 8.7.3.3, *Error Response Codes*) that may be returned in response to a received WPAC message. Both the WSP Gateway and the NAADS WPA Gateway use this element in Error messages. Multiple instances may occur within a single <WPAC_attributes> block. Each occurrence of the WPAC_responseCode element should have a corresponding occurrence of the WPAC_note element.
WPAC_note	C	Required for Error WPAC message type. May also be optionally used in Alert, Update, or Cancel messages from the NAADS WPA Gateway to the WSP Gateway. Multiple instances may occur within a single <WPAC_attributes> block to correspond to multiple occurrences of WPAC_responseCode. The note included in this element corresponds to the WPAC_responseCode. The NAADS WPA Gateway may use the CAP-CP note element to populate this element in messages from the NAADS WPA Gateway to the WSP Gateway.
WPAC_CAPCPIdentifier	C	Required for Alert, Update, and Cancel WPAC message types. This element contains the identifier field of the CAP-CP message. Specified by the NAADS WPA Gateway.

WPAC Element	Mandatory/ Optional/ Conditional	WPAC Definition
WPAC_CAPCPSent	C	Required for Alert, Update, and Cancel WPAC message types. This element contains the sent date and time of the alert message as specified in the corresponding CAP-CP message received at the NAADS WPA Gateway. Specified by the NAADS WPA Gateway. The NAADS WPA Gateway uses CAP-CP sent element to populate this element.

8.3.2 WPAC_info Segment Element Definition

The following table contains the definition of the elements of the WPAC_info segment. The WPAC_info Segment is a required in all Alert Message, Update Message and WPA System Test Message WPAMs processed across the WPAC.

Table 10: WPAC_info Segment Element Definition

WPAC Element	Mandatory/ Optional/ Conditional	WPAC Definition
WPAC_info	C	(1) Surrounds WPAC alert info segment sub-elements. (2) Only a single occurrence is permitted within a single <WPAC_attributes>. (3) In addition to the specified sub-elements, may contain one or more <WPAC_area> blocks.
WPAC_category	C	NAADS WPA Gateway uses the CAP-CP category element to populate this element. Code Values used by WSP Gateway only: "**Geo**" - Geophysical (inc. landslide). "**Met**" - Meteorological (inc. flood). "**Safety**" - General emergency and public safety. "**Security**" - Law enforcement, military, homeland and local/private security. "**Rescue**" - Rescue and recovery. "**Fire**" - Fire suppression and rescue. "**Health**" - Medical and public health. "**Env**" - Pollution and other environmental. "**Transport**" - Public and private transportation. "**Infra**" - Utility, telecommunication, other non-transport infrastructure. "**CBRNE**" – Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack. "**Other**" - Other events.
WPAC_eventCode	M	NAADS WPA Gateway uses the CAP-CP eventCode element to populate this element. For use by the WSP for logging purposes only

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	WPAC DEFINITION
WPAC_responseType	O	NAADS WPA Gateway uses the CAP-CP responseType element to populate this element. Code values: "**Shelter**" – Take shelter in place. "**Evacuate**" – Relocate. "**Prepare**" – Make preparations. "**Execute**" – Execute a pre-planned activity. "**Monitor**" – Attend to information sources. "**Avoid**" – Avoid hazard. "**Assess**" – Evaluate the information in this message. (This value should not be used in public warning applications.) **"AllClear"** – The subject event no longer poses a threat or concern. "**None**" – No action recommended.
WPAC_severity	C	NAADS WPA Gateway uses the CAP-CP severity element to populate this element. Code Values sent to the mobile device: "**Extreme**" - Extraordinary threat to life or property. "**Severe**" - Significant threat to life or property. **"Moderate"** – Possible threat to life or property. **"Minor"** – Minimal to no known threat to life or property. **"Unknown"** – Severity unknown.
WPAC_urgency	C	NAADS WPA Gateway uses the CAP-CP urgency element to populate this element. Code Values sent to the mobile device: "**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.
WPAC_certainty	C	NAADS WPA Gateway uses the CAP-CP certainty element to populate this element. Code Values sent to the mobile device: "**Observed**" – Determined to have occurred or to be ongoing. "**Likely**" - Likely (probability > ~50%). **"Possible"** - Possible but not likely (probability <= ~50%). **"Unlikely"** – Not expected to occur (probability ~0). **"Unknown"** – Certainty unknown.
WPAC_expires	C	The expiry time of the information of the alert message for use by the WSP Gateway. The date and time is represented in UTC [dateTime] format. Maximum duration is specified in Annex B, Configurable Parameters. Specified by the NAADS WPA Gateway. For Alert and Update Messages, the value is derived from the CAP-CP expires element.

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	WPAC DEFINITION
WPAC_senderName	O	Optional element for logging purposes at the WSP Gateway. The human-readable name of the agency or authority issuing this alert. For Alert and Update Messages, the NAADS WPA Gateway uses the CAP-CP senderName element to populate this element. For WPA System Test Messages, the NAADS WPA Gateway uses the name or other identification of the WPA System Test initiator at the NAADS WPA Gateway to populate this element.
WPAC_language	C	Specifies the language of the text in the WPAC_description, for use by the mobile device. Code Values: "**English**" "**French**" **"English and French"**[18] The "English and French" value should be used by the NAADS Alert Gateway for any language in a WPAM to ensure appropriate processing in CBS.
WPAC_descriptionLength	C	The length, in characters of the text in the WPAC_description.
WPAC_description	C	The text of the alert message for use by the mobile device.

[18] For a bilingual message, the WPAC_description message contains the English-language text and the French-language text separated by demarcation symbols as defined in the latest approved National Public Alerting System's Common Look and Feel (CLF) Guidance. Either the English-language text or the French-language text may occur first.

8.3.3 WPAC_area Segment Element Definition

The following table contains the definition of the elements of the WPAC_area segment. The WPAC_area Segment is required in all Alert Message, Update Message and WPA System Test Message WPAMs processed across the WPAC.

Table 11: WPAC_area Segment Element Definition

WPAC Element	Mandatory/ Optional/ Conditional	WPAC Definition
WPAC_area	C	The aggregate of WPAM spatial elements including the WPAC_geocode, WPAC_polygon, WPAC_circle. Multiple occurrences permitted, in which case the target area for the <WPAC_area> block is the union of all the included <WPAC_area> elements. The WPAC_area segment may contain one or multiple instances of <WPAC_geocode> but only a single instance of a <WPAC_polygon> or <WPAC_circle>. If multiple <WPAC_geocode> elements are included, the area described by this <WPAC_area> is the union of the <WPAC_geocode> elements. The WSP targeting policies are beyond the scope of this Specification. The WPAC Area Segment shall contain, at a minimum, a WPAC_polygon element or WPAC_circle element with corresponding values.
WPAC_areaDesc	C	The text describing the affected area of the alert message for use by the WSP for logging purposes only. NAADS WPA Gateway uses the CAP-CP areaDesc element to populate this element.
WPAC_polygon	C	The paired values of points defining a polygon that delineates the affected area of the alert message. NAADS WPA Gateway uses the CAP-CP polygon element to populate this element. A maximum of 150 paired values of points (i.e., latitude/longitude pairs) per WPAC_polygon element may be specified in the polygon. When a polygon is used, the geographical coordinates associated with the polygon will supersede and be used in place of the geographical coordinates associated with the geocode.
WPAC_circle	C	The paired values of a point and radius delineating the affected area of the alert message. NAADS WPA Gateway uses the CAP-CP circle element to populate this element. When a circle is used, the geographical coordinates associated with the circle will supersede and be used in place of the geographical coordinates associated with the geocode.

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	WPAC DEFINITION
WPAC_geocode	C	The geographic code delineating the affected area of the alert message. The WPAC_geocode is populated directly by originating CAP-CP geocode [Ref 40] that identifies the affected area within Canada for the alert message. By default, the geocode shall automatically populate the WPAC_polygon element (see above) with geo-coordinates unless the Alert Issuer has further defined a more granular polygon or circle to more accurately delineate the affected alert area. WPAC-geocode may contain multiple geocodes to define a larger alerting area that is an aggregate of the geocodes.

8.3.4 Definition of WPAC_signature Segment Element Definition

Table 12: WPAC_signature Element Definition

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	WPAC DEFINITION
WPAC_signature	O	The NAADS WPA Gateway may forward a Digital_signature element and corresponding value to the WSP Gateway for an Alert, Update, Cancel or WPA Test Message. Digital Signatures shall not be included with Ack, Error or Link Test Messages. The WSP Gateway shall not authenticate or validate the Digital Signature. However, the WSP Gateway shall archive this element should future validation be required.

8.4 WPAC Message XML Definition

The following is the XML scheme definition for the WPAC messages transmitted across the C-Interface:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
    targetNamespace = "wpac:1.0"
    xmlns:wpac = "wpac:1.0"
    xmlns:xs = "http://www.w3.org/2001/XMLSchema"
    elementFormDefault = "qualified"
    attributeFormDefault = "unqualified">
    <element name = "WPAC_attributes">
    <annotation>
       <documentation>WPAC Alert Message (version 1.0)</documentation>
    </annotation>
    <complexType>
        <sequence>
```

```
<element name = "WPAC_version" type = "string"/>
<element name = "WPAC_gatewayID" type = "anyURI"/>
<element name = "WPAC_identifier">
   <simpleType>
      <restriction base = "hexBinary">
         <length value = "4" fixed = "true" />
      </restriction>
   </simpleType>
</element>
<element name = "WPAC_referencedIdentifier" minOccurs="0">
    <simpleType>
      <restriction base = "hexBinary">
         <length value = "4" fixed = "true" />
      </restriction>
   </simpleType>
</element>
<element name = "WPAC_referencedIdentifierCAPCP" type = "string"
    minOccurs = "0"/>
<element name = "WPAC_deliveryChannel" minOccurs = "0">
   <simpleType>
      <restriction base = "string">
         <enumeration value = "Mandatory Public"/>
         <enumeration value = "Invisible Test"/>
      </restriction>
   </simpleType>
</element>
<element name = "WPAC_sender" type = "string" minOccurs = "0"/>
<element name = "WPAC_sent" type = "dateTime"/>
<element name = "WPAC_status">
   <simpleType>
      <restriction base = "string">
         <enumeration value = "Actual"/>
         <enumeration value = "System"/>
      </restriction>
   </simpleType>
</element>
<element name = "WPAC_msgType">
   <simpleType>
      <restriction base = "string">
         <enumeration value = "Alert"/>
         <enumeration value = "Update"/>
```

```
            <enumeration value = "Cancel"/>
            <enumeration value = "Ack"/>
            <enumeration value = "Error"/>
            <enumeration value = "WPAS Test"/>
            <enumeration value = "Link Test"/>
            <enumeration value = "Transmission Control - Cease"/>
            <enumeration value = "Transmission Control - Resume"/>
         </restriction>
      </simpleType>
   </element>
   <element name = "WPAC_responseCode" type = "string" minOccurs = "0"
      maxOccurs = "unbounded"/>
   <element name = "WPAC_note" type = "string" minOccurs = "0"
      maxOccurs = "unbounded"/>
   <element name = "WPAC_CAPCPIdentifier" type = "string" minOccurs = "0"/>
   <element name = "WPAC_CAPCPSent" type = "dateTime" minOccurs = "0"/>
   <element name = "WPAC_info" minOccurs = "0">
      <complexType>
         <sequence>
            <element name = "WPAC_category">
               <simpleType>
                  <restriction base = "string">
                     <enumeration value = "Geo"/>
                     <enumeration value = "Met"/>
                     <enumeration value = "Safety"/>
                     <enumeration value = "Security"/>
                     <enumeration value = "Rescue"/>
                     <enumeration value = "Fire"/>
                     <enumeration value = "Health"/>
                     <enumeration value = "Env"/>
                     <enumeration value = "Transport"/>
                     <enumeration value = "Infra"/>
                     <enumeration value = "CBRNE"/>
                     <enumeration value = "Other"/>
                  </restriction>
               </simpleType>
            </element>
            <element name = "WPAC_eventCode" type = “string“ />
            <element name = "WPAC_responseType" minOccurs = "0">
               <simpleType>
                  <restriction base = "string">
```

```
            <enumeration value = "Shelter"/>
            <enumeration value = "Evacuate"/>
            <enumeration value = "Prepare"/>
            <enumeration value = "Execute"/>
            <enumeration value = "Monitor"/>
            <enumeration value = "Avoid"/>
            <enumeration value = "Assess"/>
            <enumeration value = "AllClear"/>
            <enumeration value = "None"/>
         </restriction>
      </simpleType>
   </element>
   <element name = "WPAC_severity">
      <simpleType>
         <restriction base = "string">
            <enumeration value = "Extreme"/>
            <enumeration value = "Severe"/>
            <enumeration value = "Moderate"/>
            <enumeration value = "Minor"/>
            <enumeration value = "Unknown"/>
            </restriction>
         </simpleType>
      </element>
      <element name = "WPAC_urgency">
         <simpleType>
            <restriction base = "string">
               <enumeration value = "Immediate"/>
               <enumeration value = "Expected"/>
               <enumeration value = "Future"/>
               <enumeration value = "Past"/>
               <enumeration value = "Unknown"/>
             </restriction>
          </simpleType>
       </element>
       <element name = "WPAC_certainty">
          <simpleType>
             <restriction base = "string">
                <enumeration value = "Observed"/>
                <enumeration value = "Likely"/>
             </restriction>
          </simpleType>
```

```
            </element>
            <element name = "WPAC_expires" type = "dateTime"/>
            <element name = "WPAC_senderName" type = "string"
               minOccurs = "0"/>
            <element name = "WPAC_language">
               <simpleType>
                  <restriction base = "string">
                     <enumeration value = "English"/>
                     <enumeration value = "French"/>
                     <enumeration value = "English and French"/>
                  </restriction>
               </simpleType>
            </element>
            <element name = "WPAC_descriptionLength" type = "integer"/>
            <element name = "WPAC_description" type = "string"/>
            <element name = "WPAC_area" minOccurs = "0"
               maxOccurs = "unbounded">
               <complexType>
                  <sequence>
                     <element name = "WPAC_areaDesc"
                        type = "string"/>
                     <element name = "WPAC_polygon" type = "string"
                        minOccurs = "0" maxOccurs = "unbounded"/>
                     <element name = "WPAC_circle" type = "string"
                        minOccurs = "0" maxOccurs = "unbounded"/>
                     <element name = "WPAC_geocode" type= "string"
                        maxOccurs = "unbounded"/>
                  </sequence>
               </complexType>
            </element>
         </sequence>
      </complexType>
      </element>
      <element name="WPAC_signature" minOccurs = "0">
         <complexType>
           <sequence>
              <any namespace="http://www.w3c.org/2000/09/xmldsig#"
              processContents="lax" maxOccurs="unbounded"/>
           </sequence>
         </complexType>
      </element>
```

```
            </sequence>
          </complexType>
        </element>
</schema>
```

8.5 WPAC Message Types & Example XML

This Section defines the XML structure and XML contents for the following types of WPAC messages including example messages for each message:

- *Alert Message*
- *Update Message*
- *Cancel Message*
- *Ack Message*
- *Error Message*
- *Link Test*
- *WPA System Test Message*
- *Transmission Control – Cease Message*
- *Transmission Control - Resume Message*

The definitions of Mandatory, Optional, and Conditional used in the element definition tables within this Section are as follows:

Mandatory (M)	This element is required.
Conditional (C)	This element may be required in the segment depending on the values of other elements.
Optional (O)	This element may or may not be included in the segment. It is not required to process a WPAM over the WPAC. However, the values associated with this element may provide additional context and reference information when archived in the CBS log and reviewed at a later date.

8.5.1 Alert Message

A WPAC Alert Message initiated by the NAADS WPA Gateway shall consist of a WPAM containing one WPAC_attributes segment, one WPAC_info segment and one or more WPAC_area segments. The WPAC_status is set to "Actual" and the WPAC_msgType is set to "Alert" to indicate the Alert Message.

The following table summarizes the required WPAC elements of the WPAC_attributes segment for an Alert Message (see *Section 8.3.1, WPAC_attributes Segment Element Definition and Table 9: WPAC_attributes Segment Element Definition* for the element encoding formats):

Table 13: Elements of Alert Attributes Segment for Alert Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_gateway	M	NAADS WPA Gateway identifier which initiated the WPAC message.
WPAC_identifier	M	WPAM identification number for this WPAC message assigned by the NAADS WPA Gateway.
WPAC_deliveryChannel	M	Specifies that the message is to be sent to the Mandatory Public Channel (MI=4370) or the Invisible Test Channel (MI=4380).
WPAC_sender	M	Identifies the originator of the alert per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_sent	M	Date and time in UTC when the Alert Message is sent by the NAADS WPA Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "Actual".
WPAC_msgType	M	Value of "Alert".
WPAC_CAPCPIdentifier	M	Specifies the identifier value in the corresponding CAP-CP message.
WPAC_CAPCPSent	M	Specifies the date and time the corresponding CAP-CP message was sent.

The following table summarizes the required WPAC elements of the WPAC_info segment for an Alert Message (see Section 8.3.2, *WPAC_info Segment Element Definition,* Table 10: WPAC_info Segment Element Definition for the element encoding formats):

Table 14: Elements of Alert Info Segment for Alert Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_category	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_eventCode	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_responseType	O	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_severity	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_urgency	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_certainty	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.

WPAC Element	Mandatory/ Optional/ Conditional	Value
WPAC_expires	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_senderName	O	Optional element which may be included per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_language	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_descriptionLength	M	Length in characters of the text message per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_description	M	Text message per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.

The following table summarizes the required WPAC elements of the WPAC_area segment for an Alert Message (see *Section 8.3.3, WPAC_area Segment Element Definition, Table 11: WPAC_area Segment Element Definition for the element encoding formats*):

Table 15: Elements of Alert Area Segment for Alert Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_areaDesc	M	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition.
WPAC_polygon	C	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition. At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all Alert Messages.
WPAC_circle	C	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition. At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all Alert Messages.
WPAC_geocode	C	Geocode indicating the updated alert area. (See Section 8.3.5, Definition of WPAC_geocode Element). At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all Alert Messages.

The following table summarizes the optional WPAC element of the WPAC_signature segment for an Alert Message (see Section 8.3.4, *WPAC_signature Segment Element Definition,* Table 12 *WPAC_signature Segment Element Definition* for the element encoding formats):

Table 16: Elements of Alert Signature Segment for Alert Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_signature	O	Per Table 12: WPAC_signature Segment Element Definition

The following is an example format of a WPAC Alert Message initiated by the NAADS WPA Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac:1.0">
  <WPAC_version>1.0</WPAC_version>
  <WPAC_gatewayID>http://naads_alert_gateway.ca</WPAC_gatewayID>
  <WPAC_identifier>000000A9</WPAC_identifier>
  <WPAC_deliveryChannel>Mandatory Public</WPAC_deliveryChannel>
  <WPAC_sender>SKVillageParadiseHillTownSt.WalburgRM#501</WPAC_sender>
  <WPAC_sent>2015-02-09T18:35:00-07:00</WPAC_sent>
```

```
  <WPAC_status>Actual</WPAC_status>
  <WPAC_msgType>Alert</WPAC_msgType>
  <WPAC_CAPCPIdentifier>B5246B86-A364-562B-DD0A-C02D53E620E2</WPAC_CAPCPIdentifier>
  <WPAC_CAPCPSent>2015-02-09T18:22:17-07:00</WPAC_CAPCPSent>
  <WPAC_info>
    <WPAC_category>Met</WPAC_category>
    <WPAC_eventCode>flashFlood</WPAC_eventCode>
    <WPAC_severity>Severe</WPAC_severity>
    <WPAC_urgency>Expected</WPAC_urgency>
    <WPAC_certainty>Likely</WPAC_certainty>
    <WPAC_expires>2015-02-09T23:15:00Z</WPAC_expires>
    <WPAC_language>English and French</WPAC_language>
    <WPAC_descriptionLength>117</WPAC_descriptionLength>
    <WPAC_description>Severe Weather Warning in this area until 4:15pm CST///Avertissement de
temps violent dans cette zone jusqu'à 16h15 CST</WPAC_description>
    <WPAC_area>
      <WPAC_areaDesc>St. Walburg Saskatchewan</WPAC_areaDesc>
      <WPAC_polygon>
        43.735824,-79.630192 43.646393,-79.6088 43.560342,-79.522959 43.633161,-79.467339
43.612914,-79.339286 43.793778,-79.113467 43.855447,-79.170316 43.735824,-
79.630192</WPAC_polygon>
          <WPAC_geocode>3520</WPAC_geocode>
        </WPAC_area>
  </WPAC_info>
<WPAC_signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="NAADS
Signature"><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>Nq9KSlWoejxKbjKUrwy2vPs7tvI=
</DigestValue></Reference></SignedInfo><SignatureValue>TiDfCfhjKLFWfTFJRCMdMXobs3RSqHWL2vAhrS
PlRtqlo1kXaEJqkogF9Asxokcom5+kVUGMd0lvrji6lyKTLcVVislKNTYXJdDpDzqe145a9FbmpO6nxBJnhNtt+qonFkO
nRhY+/UD4FKtXMtGQpy/IvT7Um3F1B6/x0s285jrsJmsOitQoSSvtLmXNESQiP8bH4Y8tUe6FojWG3PvOMKapsUMnx1f2
2naMJdEkiCNEC9PODbxtYwz5ODdXM/EJKnDNy8Mqgho0AzdrGuOt3oZbKs3h4J94I9PdOo6sPnDFxA7qSmFVqLqzPs+v4
KSjCpf+LHix3vPVuR20zc0E0w==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIF0jCCBLqgA
wIBAgIQQ4q3qW4

…

WAZEmJ2Y55X+ovjANBgkqhkiG9w0BAQUFADCBtTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDjEx6vUJDGBvx2m5Af4CA592
4Mfh2xsCLYulSKaHkNV8P+gKdV0+zjrajosbOSDiVWY34Qmvj24JEKLETZFI+AVOSWN559PKKEvT7SirDdFqP0OaD1HV0
5bes65M+LJ</X509Certificate></X509Data></KeyInfo></WPAC_signature>

</WPAC_attributes>
```

This WPA Alert Message would be broadcast as:

> Severe Weather Warning in this area until 4:15pm CST///Avertissement de temps violent dans cette zone jusqu'à 16h15 CST

8.5.2 Update Message

A WPAC Update Message shall consist of a WPAM containing one WPAC_attributes segment, one WPAC_info segment and one or more WPAC_area segments. The WPAC_status is set to "Actual" and the WPAC_msgType is set to "Update" to indicate the Update Message, with the <WPAC_referencedIdentifier> containing the WPAM identification number for the message to be updated.

The following table summarizes the required WPAC elements of the WPAC_attributes segment for an Update Message (see *Section 8.3.1, WPAC_attributes Segment Element Definition, Table 9: WPAC_attributes Segment Element Definition* for the element encoding formats):

Table 17: Elements of Alert Attributes Segment for Update Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_gatewayID	M	NAADS WPA Gateway identifier which initiated the WPAC message.
WPAC_identifier	M	WPAM identification number for this WPAC message assigned by the NAADS WPA Gateway. Note: To uniquely identify a message, the WSP Gateway uses the WPAC_identifier in conjunction with the WPAC_CAPCPIdentifier.
WPAC_referencedIdentifier	M	WPAM identification number of the corresponding message to be updated.
WPAC_referencedIdentifierCAPCP	M	Identifier of the corresponding CAP-CP message of the corresponding alert message to be updated.
WPAC_deliveryChannel	M	Specifies that the message is to be sent to the Mandatory Public Channel (MI=4370) or the Invisible Test Channel (MI=4380).
WPAC_sender	M	Identifies the originator of the alert update per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_sent	M	Date and time in UTC when the Update Message is sent by the NAADS WPA Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "Actual".
WPAC_msgType	M	Value of "Update".
WPAC_CAPCPIdentifier	M	Specifies the identifier value in the corresponding CAP-CP message.
WPAC_CAPCPSent	M	Specifies the date and time the corresponding CAP-CP message was sent.

The following table summarizes the required WPAC elements of the WPAC_info segment for an Update Message (see *Section 8.3.2, WPAC_info Segment Element Definition, Table 10: WPAC_info Segment Element Definition* for the element encoding formats):

Table 18: Elements of Alert Info Segment for Update Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_category	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_eventCode	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_responseType	O	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2 WPAC_info Segment Element Definition.
WPAC_severity	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_urgency	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_certainty	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_expires	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_senderName	O	Optional element which may be included per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_language	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_descriptionLength	M	Length in characters of the text message per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_description	M	Text message per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.

The following table summarizes the required WPAC elements of the WPAC_area segment for an Update Message (see *Section 8.3.3, WPAC_area Segment Element Definition, Table 11: WPAC_area Segment Element Definition* for the element encoding formats):

Table 19: Elements of Alert Area Segment for Update Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_areaDesc	M	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition.
WPAC_polygon	C	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition. At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all Update Messages.

WPAC Element	Mandatory/ Optional/ Conditional	Value
WPAC_circle	C	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition. At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all Update Messages.
WPAC_geocode	C	Geocode indicating the updated alert area. (See Section 8.3.5, Definition of WPAC_geocode Element). At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all Update Messages. The updated alert area may be different than the alert area of the message being updated.

The following table summarizes the optional WPAC element of the WPAC_signature segment for an Update Message (see *Section 8.3.4, WPAC_signature Segment Element Definition, Table 12 WPAC_signature Segment Element Definition* for the element encoding formats):

Table 20: Elements of Alert Signature Segment for Update Message

WPAC Element	Mandatory/ Optional/ Conditional	Value
WPAC_signature	O	Per Table 12: *WPAC_signature Segment Element Definition*

The following is an example format of an Update Message initiated by the NAADS WPA Gateway. In this example, the Alert Message example of *Section 8.5.1, Alert Message,* has been updated with a new expiration time of 8:15pm:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac: 1.0">
   <WPAC_version>1.0</WPAC_version>
   <WPAC_gatewayID>http://naads_alert_gateway.ca</WPAC_gatewayID>
   <WPAC_identifier>000000AA</WPAC_identifier>
   <WPAC_referencedIdentifier>000000A9</WPAC_referencedIdentifier>
   <WPAC_referencedIdentifierCAPCP>B5246B86-A364-562B-DD0A-
C02D53E620E2</WPAC_referencedIdentifierCAPCP>
   <WPAC_deliveryChannel>Mandatory Public</WPAC_deliveryChannel>
   <WPAC_sender>SKVillageParadiseHillTownSt.WalburgRM#501</WPAC_sender>
   <WPAC_sent>2015-02-09T18:57:00-07:00</WPAC_sent>
   <WPAC_status>Actual</WPAC_status>
   <WPAC_msgType>Update</WPAC_msgType>
   <WPAC_CAPCPIdentifier>8747CFDB-E069-9BB6-9D42-20DEF2E29635</WPAC_CAPCPIdentifier>
   <WPAC_CAPCPSent>2015-02-09T18:57:00-07:00</WPAC_CAPCPSent>
   <WPAC_info>
```

```
      <WPAC_category>Met</WPAC_category>
      <WPAC_eventCode>flashFlood</WPAC_eventCode>
      <WPAC_severity>Severe</WPAC_severity>
      <WPAC_urgency>Expected</WPAC_urgency>
      <WPAC_certainty>Likely</WPAC_certainty>
      <WPAC_expires>2015-02-10T03:15:00Z</WPAC_expires>
      <WPAC_language>English and French</WPAC_language>
      <WPAC_descriptionLength>117</WPAC_descriptionLength>
      <WPAC_description>Severe Weather Warning in this area until 8:15pm CST///Avertissement
de temps violent dans cette zone jusqu'à 20h15 CST</WPAC_description>
      <WPAC_area>
         <WPAC_areaDesc>St. Walburg Saskatchewan</WPAC_areaDesc>
         <WPAC_polygon>43.735824,-79.630192 43.646393,-79.6088 43.560342,-79.522959
43.633161,-79.467339 43.612914,-79.339286 43.793778,-79.113467 43.855447,-79.170316
43.735824,-79.630192</WPAC_polygon>
         <WPAC_geocode>3520</WPAC_geocode>
      </WPAC_area>
   </WPAC_info>
<WPAC_signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="NAADS
Signature"><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>Nq9KSlWoejxKbjKUrwy2vPs7tvI=
</DigestValue></Reference></SignedInfo><SignatureValue>TiDfCfhjKLFWfTFJRCMdMXobs3RSqHWL2vAhrS
PlRtqlo1kXaEJqkogF9Asxokcom5+kVUGMd0lvrji6lyKTLcVVislKNTYXJdDpDzqe145a9FbmpO6nxBJnhNtt+qonFkO
nRhY+/UD4FKtXMtGQpy/IvT7Um3F1B6/x0s285jrsJmsOitQoSSvtLmXNESQiP8bH4Y8tUe6FojWG3PvOMKapsUMnx1f2
2naMJdEkiCNEC9PODbxtYwz5ODdXM/EJKnDNy8Mqgho0AzdrGuOt3oZbKs3h4J94I9PdOo6sPnDFxA7qSmFVqLqzPs+v4
KSjCpf+LHix3vPVuR20zc0E0w==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIF0jCCBLqgA
wIBAgIQQ4q3qW4
…
WAZEmJ2Y55X+ovjANBgkqhkiG9w0BAQUFADCBtTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDjEx6vUJDGBvx2m5Af4CA592
4Mfh2xsCLYulSKaHkNV8P+gKdV0+zjrajosbOSDiVWY34Qmvj24JEKLETZFI+AVOSWN559PKKEvT7SirDdFqP0OaD1HV0
5bes65M+LJ</X509Certificate></X509Data></KeyInfo></WPAC_signature>
</WPAC_attributes>
```

8.5.3 Cancel Message

A WPAC Cancel Message shall consist of a WPAM containing one WPAC_attributes segment. The WPAC_status is set to "Actual" and the WPAC_msgType is set to "Cancel" to indicate the Cancel Message, with the <WPAC_referencedIdentifier> containing the WPAM identification number for the message to be cancelled.

The following table summarizes the required WPAC elements of the WPAC_attributes segment for an Alert Cancel Message (see *Section 8.3.1, WPAC_attributes Segment Element Definition, Table 9: WPAC_attributes Segment Element Definition* for the element encoding formats):

Table 21: Elements of Alert Attributes Segment for Cancel Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_gatewayID	M	NAADS WPA Gateway identifier which initiated the WPAC message.
WPAC_identifier	M	WPAM identification number for this WPAC message assigned by the NAADS WPA Gateway. Note: To uniquely identify a message, the WSP Gateway uses the WPAC_identifier in conjunction with the WPAC_CAPCPIdentifier.
WPAC_referencedIdentifier	M	WPAM identification number of the corresponding message to be cancelled.
WPAC_referencedIdentifierCAPCP	M	Identifier of the corresponding CAP-CP message of the corresponding alert message to be cancelled.
WPAC_sender	M	Identifies the originator of the alert cancellation per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_sent	M	Date and time in UTC when the Cancel Message is sent by the NAADS WPA Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "Actual".
WPAC_msgType	M	Value of "Cancel".
WPAC_CAPCPIdentifier	M	Specifies the identifier value in the corresponding CAP-CP message.
WPAC_CAPCPSent	M	Specifies the date and time the corresponding CAP-CP message was sent.

The following table summarizes the optional WPAC element of the WPAC_signature segment for an Alert Cancel Message (see *Section 8.3.4, WPAC_signature Segment Element Definition, Table 12 WPAC_signature Segment Element Definition* for the element encoding formats):

Table 22: Elements of Alert Signature Segment for Cancel Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_signature	O	Per Table 12: *WPAC_signature Segment Element Definition*

The following is an example format of an Alert Cancel Message initiated by the NAADS WPA Gateway. In this example, the Alert Message example of *Section 8.5.1, Alert Message,* has been cancelled:

```
<?xml version = "1.0" encoding = "UTF-8"?>

<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac: 1.0">

   <WPAC_version>1.0</WPAC_version>
```

```
   <WPAC_gatewayID>http://naads_alert_gateway.ca</WPAC_gatewayID>
   <WPAC_identifier>000000AB</WPAC_identifier>
   <WPAC_referencedIdentifier>000000AA</WPAC_referencedIdentifier>
 <WPAC_referencedIdentifierCAPCP>2.49.0.1.124.aaf25ef5.2015</WPAC_referencedIdentifierCAPCP>
   <WPAC_sender>SKVillageParadiseHillTownSt.WalburgRM#501</WPAC_sender>
   <WPAC_sent>2015-02-09T20:07:00-07:00</WPAC_sent>
   <WPAC_status>Actual</WPAC_status>
   <WPAC_msgType>Cancel</WPAC_msgType>
   <WPAC_CAPCPIdentifier>2.49.0.1.124.aaf25ef8.2015</WPAC_CAPCPIdentifier>
   <WPAC_CAPCPSent>2015-02-09T20:07:00-07:00</WPAC_CAPCPSent>
<WPAC_signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="NAADS
Signature"><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>Nq9KSlWoejxKbjKUrwy2vPs7tvI=
</DigestValue></Reference></SignedInfo><SignatureValue>TiDfCfhjKLFWfTFJRCMdMXobs3RSqHWL2vAhrS
PlRtqlo1kXaEJqkogF9Asxokcom5+kVUGMd0lvrji6lyKTLcVVislKNTYXJdDpDzqe145a9FbmpO6nxBJnhNtt+qonFkO
nRhY+/UD4FKtXMtGQpy/IvT7Um3F1B6/x0s285jrsJmsOitQoSSvtLmXNESQiP8bH4Y8tUe6FojWG3PvOMKapsUMnx1f2
2naMJdEkiCNEC9PODbxtYwz5ODdXM/EJKnDNy8Mqgho0AzdrGuOt3oZbKs3h4J94I9PdOo6sPnDFxA7qSmFVqLqzPs+v4
KSjCpf+LHix3vPVuR20zc0E0w==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIF0jCCBLqgA
wIBAgIQQ4q3qW4

…

WAZEmJ2Y55X+ovjANBgkqhkiG9w0BAQUFADCBtTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDjEx6vUJDGBvx2m5Af4CA592
4Mfh2xsCLYulSKaHkNV8P+gKdV0+zjrajosbOSDiVWY34Qmvj24JEKLETZFI+AVOSWN559PKKEvT7SirDdFqP0OaD1HV0
5bes65M+LJ</X509Certificate></X509Data></KeyInfo></WPAC_signature>

</WPAC_attributes>
```

8.5.4 Ack Message

The WPAC Ack Message contains only a WPAC_attributes segment. In the Ack Message, the sending Gateway shall provide the identifier of that Gateway in the WPAC_gatewayID element, and indicate the time the message is acknowledged in the WPAC_sent element. The WPAC_referencedIdentifier shall contain the WPAM identification number of the message which is being acknowledged and the WPAC_status element shall indicate this is a "System" message.

The following table summarizes the required WPAC elements for an Ack Message (see *Section 8.3.1, WPAC_attributes Segment Element Definition, Table 9: WPAC_attributes Segment Element Definition* for the element encoding formats):

Table 23: Elements of Alert Attributes Segment for Ack Message

WPAC Element	Mandatory/ Optional/ Conditional	Value
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_gatewayID	M	WSP Gateway identifier or NAADS WPA Gateway Identifier.
WPAC_identifier	M	WPAM identification number assigned by the sending Gateway.

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_referencedIdentifier	M	The WPAM identification number value contained in the WPAC message received from the sending Gateway which is being acknowledged.
WPAC_sent	M	Date and time in UTC when the ACK Message is sent by the NAADS WPA Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "System".
WPAC_msgType	M	Value of "Ack".

The following is the format of an example Ack Message from the WSP Gateway to the NAADS WPA Gateway upon receipt of a WPA Alert, Update, or Cancel message:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac: 1.0">
   <WPAC_version>1.0</WPAC_version>
   <WPAC_gatewayID>http://wpas_wsp_alert_gateway_uri</WPAC_gatewayID>
   <WPAC_identifier>000000B5</WPAC_identifier>
   <WPAC_referencedIdentifier>000000B4</WPAC_referencedIdentifier>
   <WPAC_sent>2015-02-17T14:57:05-07:00</WPAC_sent>
   <WPAC_status>System</WPAC_status>
   <WPAC_msgType>Ack</WPAC_msgType>
</WPAC_attributes>
```

8.5.5 Error Message

The WPAC Error Message contains only a WPAC_attributes segment. An error condition is indicated by the WPAC_msgType element containing "Error" with one or more WPAC_responseCode elements containing response codes and with one or more WPAC_note elements containing WPAC response descriptions (see *Section 8.7.3.3, Error Response Codes*).

The following table summarizes the required WPAC elements for a WSP Gateway error indication of a NAADS WPA Gateway-initiated Alert, Update or Cancel message (see *Section 8.3.1, WPAC_attributes Segment Element Definition, Table 9: WPAC_attributes Segment Element Definition* for the element encoding format):

Table 24: Elements of Alert Attributes Segment for Error Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_gatewayID	M	WSP Gateway identifier or NAADS WPA Gateway Identifier.
WPAC_identifier	M	WPAM identification number assigned by the sending Gateway.

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_referencedIdentifier	M	The WPAM identification number value contained in the WPAC message received from the sending Gateway which is being sent an error response.
WPAC_sent	M	Date and time in UTC when the Error Message is sent by the NAADS WPA Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "System".
WPAC_msgType	M	Value of "Error".
WPAC_responseCode	M	WPAC response code from Section 8.7.3.3, Error Response Codes. Multiple occurrences of the WPAC_responseCode may occur in this error response.
WPAC_note	M	WPAC Response description from Section 8.7.3.3, Error Response Codes. Multiple occurrence of the WPAC_note may occur in this error response.

The following is the format of an example WSP Gateway error message sent from the WSP Gateway to the NAADS WPA Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac: 1.0">
   <WPAC_version>1.0</WPAC_version>
   <WPAC_gatewayID>http://wpas_wsp_gateway_uri</WPAC_gatewayID>
   <WPAC_identifier>000000B5</WPAC_identifier>
   <WPAC_referencedIdentifier>000000B4</WPAC_referencedIdentifier>
   <WPAC_sent>2015-02-25T14:50:05-07:00</WPAC_sent>
   <WPAC_status>System</WPAC_status>
   <WPAC_msgType>Error</WPAC_msgType>
   <WPAC_responseCode>104</WPAC_responseCode>
   <WPAC_note>invalid-element WPAC_expires_date_time</WPAC_note>
</WPAC_attributes>
```

The above example indicates the WSP Gateway received the Alert or Update message after the message expiration time.

The following is the format of an example Link Test error message with multiple error conditions reported, sent from the WSP Gateway to the NAADS WPA Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac: 1.0">
   <WPAC_version>1.0</WPAC_version>
```

```
   <WPAC_gatewayID>http://wpas_wsp_gateway_uri</WPAC_gatewayID>
   <WPAC_identifier>000000B2</WPAC_identifier>
   <WPAC_referencedIdentifier>000000B1</WPAC_referencedIdentifier>
   <WPAC_sent>2008-06-25T14:50:05-07:00</WPAC_sent>
   <WPAC_status>System</WPAC_status>
   <WPAC_msgType>Error</WPAC_msgType>
   <WPAC_responseCode>104</WPAC_responseCode>
   <WPAC_responseCode>105</WPAC_responseCode>
   <WPAC_note>invalid-element WPAC_sent</WPAC_note>
   <WPAC_note>missing-element WPAC_status</WPAC_note>
</WPAC_attributes>
```

The above example indicates the WSP Gateway is returning an error response to the NAADS WPA Gateway for multiple error conditions. The first occurrence of the WPAC_responseCode element is associated with the first occurrence of the WPAC_note element and the second occurrence of the WPAC_responseCode element is associated with the second occurrence of the WPAC_note element.

8.5.6 Link Test Message

The Link Test Message shall be a WPAC message containing only a WPAC_attributes segment. A Link Test Message shall be indicated by a WPAC_status element with as value of "System" and a WPAC_msgType element value of "Link Test". The sending Gateway shall indicate the time the message was initiated in the WPAC_sent element. The sending Gateway shall assign a unique WPAM identification number to the Link Test Message, specified in the WPAC_identifier element.

The following table summarizes the required WPAC elements for a Link Test Message (see *Section 8.3.1, WPAC_attributes Segment Element Definition, Table 9: WPAC_attributes Segment Element Definition* for the encoding formats):

Table 25: Elements of Alert Attributes for a Link Test Message

Segment for Link Test Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_gatewayID	M	WSP Gateway or NAADS WPA Gateway identifier.
WPAC_identifier	M	WPAM identification number assigned by the sending Gateway.
WPAC_sent	M	Date and time in UTC when the Link Test Message is sent by the NAADS WPA Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "System".
WPAC_msgType	M	Value of "Link Test".

The following is an example of the format for a Link Test Message initiated from the NAADS WPA Gateway and sent to the WSP Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac: 1.0">
   <WPAC_version>1.0</WPAC_version>
   <WPAC_gatewayID>http://naads_alert_gateway.ca</WPAC_gatewayID>
   <WPAC_identifier>000000B1</WPAC_identifier>
   <WPAC_sent>2015-02-25T14:50:00-07:00</WPAC_sent>
   <WPAC_status>System</WPAC_status>
   <WPAC_msgType>Link Test</WPAC_msgType>
</WPAC_attributes>
```

8.5.7 WPA System Test Message

The NAADS WPA Gateway may issue a WPA System Test Message to the WSP Gateway over the C-Interface (see Section 7.3, WPA System Test *Call Flow*). The WPA System Test Message shall be a WPAM containing a WPAC_attributes segment, one WPAC_info segment, and one or more WPAC_area segments.

A WPA System Test Message shall be indicated by a WPAC_status element with a value of "System", and a WPAC_msgType element value of "WPAS Test". The NAADS WPA Gateway shall assign a unique WPAM identification number to the WPA System Test Message, specified in the WPAC_identifier element.

The following table summarizes the required WPAC elements of the WPAC_attributes segment for a NAADS WPA Gateway-initiated WPA System Test Message (see *Section 8.3.1, WPAC_attributes Segment Element Definition, Table 9: WPAC_attributes Segment Element Definition* for the element encoding format):

Table 26: Elements of Alert Attributes Segment for WPA System Test Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_gatewayID	M	NAADS WPA Gateway identifier.
WPAC_identifier	M	WPAM identification number assigned by the NAADS WPA Gateway.
WPAC_deliveryChannel	M	Specifies that the message is to be sent to the Mandatory Public Channel (MI=4370) or the Invisible Test Channel (MI=4380).
WPAC_sent	M	Date and time in UTC when the WPA System Test Message is sent by the NAADS WPA Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "System".
WPAC_msgType	M	Value of "WPAS Test".

The following table summarizes the required WPAC elements of the WPAC_info segment for a NAADS WPA Gateway-initiated WPA System Test Message (see *Section 8.3.2, WPAC_info Segment Element Definition, Table 10: WPAC_info Segment Element Definition* for the element encoding format):

Table 27: Elements of Alert Info Segment for WPA System Test Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_category	M	Value of "Other".
WPAC_eventCode	M	Value of "testMessage".
WPAC_severity	M	Value of "Severe".
WPAC_urgency	M	Value of "Expected".
WPAC_certainty	M	Value of "Likely".
WPAC_expires	M	Date and time in UTC when the WPA System Test Message is to expire the NAADS WPA Gateway in ISO 8601 date and time format.[Ref 43], (To be determined by the NAAD System Administrator).
WPAC_senderName	O	Indicates the name or other identification of the WPA System Test initiator at the NAADS WPA Gateway. May be used for WSP Gateway logging purposes only.
WPAC_language	M	Per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.
WPAC_descriptionLength	M	Length in characters of the text message.
WPAC_description	M	Text message per Table 10: WPAC_info Segment Element Definition of Section 8.3.2, WPAC_info Segment Element Definition.

The following table summarizes the required WPAC elements of the WPAC_area segment for a WPA System Test Message (see *Section 8.3.3, WPAC_area Segment Element Definition, Table 11: WPAC_area Segment Element Definition* for the element encoding formats):

Table 28: Elements of Alert Area Segment for WPA System Test Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_areaDesc	M	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition.
WPAC_polygon	C	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition. At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all WPA System Test Messages.
WPAC_circle	C	Per Table 11: WPAC_area Segment Element Definition of Section 8.3.3, WPAC_area Segment Element Definition. At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all WPA System Test Messages.

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_geocode	C	Geocode indicating the WPA System Test area. At a minimum, there must be a populated WPAC_polygon or WPAC_circle and/or WPAC-geocode for all WPA System Test Messages.

The following table summarizes the optional WPAC element of the WPAC_signature segment for a WPA System Test Message (see *Section 8.3.4, WPAC_signature Segment Element Definition, Table 12 WPAC_signature Segment Element Definition* for the element encoding formats):

Table 29: Elements of Alert Signature Segment for WPA System Test Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_signature	O	Per Table 12: *WPAC_signature Segment Element Definition*

The following is an example of the format for a WPA System Test Message initiated from the NAADS WPA Gateway and sent to the WSP Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac: 1.0">
   <WPAC_version>1.0</WPAC_version>
   <WPAC_gatewayID>http://naads_alert_gateway.ca</WPAC_gatewayID>
   <WPAC_identifier>000000B3</WPAC_identifier>
   <WPAC_deliveryChannel>Invisible Test</WPAC_deliveryChannel>
   <WPAC_sent>2015-02-25T14:50:00-07:00</WPAC_sent>
   <WPAC_status>System</WPAC_status>
   <WPAC_msgType>WPAS Test</WPAC_msgType>
   <WPAC_info>
      <WPAC_category>Other</WPAC_category>
      <WPAC_eventCode>testMessage</WPAC_eventCode>
      <WPAC_severity>Severe</WPAC_severity>
      <WPAC_urgency>Expected</WPAC_urgency>
      <WPAC_certainty>Likely</WPAC_certainty>
      <WPAC_expires>2015-02-09T23:15:00Z</WPAC_expires>
      <WPAC_senderName>John Doe</WPAC_senderName>
      <WPAC_language>English and French</WPAC_language>
      <WPAC_descriptionLength>202</WPAC_descriptionLength>
      <WPAC_description>TEST - This is a scheduled TEST of the Ontario Public Alerting System
- No action is required///TEST - Il s'agit d'un essai prévu du système d'alerte au public de
l'Ontario - Aucune mesure n'est nécessaire</WPAC_description>
```

```
      <WPAC_area>
         <WPAC_areaDesc>St. Walburg Saskatchewan</WPAC_areaDesc>
         <WPAC_polygon>43.735824,-79.630192 43.646393,-79.6088 43.560342,-79.522959
43.633161,-79.467339 43.612914,-79.339286 43.793778,-79.113467 43.855447,-79.170316
43.735824,-79.630192</WPAC_polygon>
         <WPAC_geocode>3520</WPAC_geocode>
      </WPAC_area>
  </WPAC_info>
<WPAC_signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="NAADS
Signature"><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>Nq9KSlWoejxKbjKUrwy2vPs7tvI=
</DigestValue></Reference></SignedInfo><SignatureValue>TiDfCfhjKLFWfTFJRCMdMXobs3RSqHWL2vAhrS
PlRtqlo1kXaEJqkogF9Asxokcom5+kVUGMd0lvrji6lyKTLcVVislKNTYXJdDpDzqe145a9FbmpO6nxBJnhNtt+qonFkO
nRhY+/UD4FKtXMtGQpy/IvT7Um3F1B6/x0s285jrsJmsOitQoSSvtLmXNESQiP8bH4Y8tUe6FojWG3PvOMKapsUMnx1f2
2naMJdEkiCNEC9PODbxtYwz5ODdXM/EJKnDNy8Mqgho0AzdrGuOt3oZbKs3h4J94I9PdOo6sPnDFxA7qSmFVqLqzPs+v4
KSjCpf+LHix3vPVuR20zc0E0w==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIF0jCCBLqgA
wIBAgIQQ4q3qW4
…
WAZEmJ2Y55X+ovjANBgkqhkiG9w0BAQUFADCBtTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDjEx6vUJDGBvx2m5Af4CA592
4Mfh2xsCLYulSKaHkNV8P+gKdV0+zjrajosbOSDiVWY34Qmvj24JEKLETZFI+AVOSWN559PKKEvT7SirDdFqP0OaD1HV0
5bes65M+LJ</X509Certificate></X509Data></KeyInfo></WPAC_signature>
</WPAC_attributes>
```

8.5.8 Transmission Control – Cease Message

Upon a maintenance command being issued or another error condition at the WSP Gateway, the WSP Gateway may issue a Transmission Control – Cease Message to the NAADS WPA Gateway over the C-Interface to cease message traffic over the C-Interface destined for that specific WSP Gateway. The Transmission Control – Cease Message shall be a WPAC message containing only a WPAC_attributes segment. A Transmission Control – Cease Message shall be indicated by a WPAC_status element with as value of "System" and a WPAC_msgType element value of "Transmission Control - Cease". The WSP Gateway shall indicate the time the message was initiated in the WPAC_sent element. The WSP Gateway shall assign a unique WPAM identification number to the Transmission Control message, specified in the WPAC_identifier element.

The following table summarizes the required WPAC elements for a WSP Gateway-initiated Transmission Control – Cease Message used to cease transmission (see *Section 8.3.1, WPAC_attributes Segment Element Definition, Table 9: WPAC_attributes Segment Element Definition* for the element encoding formats):

Table 30: Elements of Alert Attributes Segment for Transmission Control – Cease Message

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1, WPAC_attributes Segment Element Definition.
WPAC_gatewayID	M	WSP Gateway identifier.

WPAC Element	Mandatory/ Optional/ Conditional	Value
WPAC_identifier	M	WPAM identification number assigned by the WSP Gateway.
WPAC_sent	M	Date and time in UTC when the Cease Message is sent by the WSP Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "System".
WPAC_msgType	M	Value of "Transmission Control - Cease".

The following is an example of the format for a Transmission Control – Cease Message initiated from the WSP Gateway and sent to the NAADS WPA Gateway to cease transmissions:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac:1.0">
   <WPAC_version>1.0</WPAC_version>
   <WPAC_gatewayID>http://wpas_wsp_gateway_uri</WPAC_gatewayID>
   <WPAC_identifier>000000B6</WPAC_identifier>
   <WPAC_sent>2015-02-25T14:50:00-07:00</WPAC_sent>
   <WPAC_status>System</WPAC_status>
   <WPAC_msgType>Transmission Control - Cease</WPAC_msgType>
</WPAC_attributes>
```

8.5.9 Transmission Control – Resume Message

Once the maintenance or error condition is cleared, the WSP Gateway shall inform the NAADS WPA Gateway that transmission of messages may resume using a Transmission Control – Resume Message indicated by a WPAC_status element with as value of "System" and a WPAC_msgType element value of "Transmission Control - Resume". The WSP Gateway shall indicate the time the message was initiated in the WPAC_sent element. The WSP Gateway shall assign a unique WPAM identification number to the Transmission Control - Resume Message, specified in the WPAC_identifier element.

The following table summarizes the required WPAC elements for a WSP Gateway-initiated Transmission Control – Resume Message used to resume transmission (see *Section 8.3.1, WPAC_attributes Segment Element Definition, Table 9: WPAC_attributes Segment Element Definition* for the element encoding formats):

Table 31: Elements of Alert Attributes Segment for Transmission Control – Resume Message

WPAC Element	Mandatory/ Optional/ Conditional	Value
WPAC_version	M	Per Table 9: WPAC_attributes Segment Element Definition of Section 8.3.1 WPAC_attributes Segment Element Definition.
WPAC_gatewayID	M	WSP Gateway identifier.
WPAC_identifier	M	WPAM identification number assigned by the WSP Gateway.

WPAC ELEMENT	MANDATORY/ OPTIONAL/ CONDITIONAL	VALUE
WPAC_sent	M	Date and time in UTC when the Resume Message is sent by the WSP Gateway in ISO 8601 date and time format.[Ref 43],
WPAC_status	M	Value of "System".
WPAC_msgType	M	Value of "Transmission Control - Resume".

The following is an example of the format for a Transmission Control – Resume Message initiated from the WSP Gateway and sent to the NAADS WPA Gateway to resume transmissions:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<WPAC_attributes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="wpac:1.0">
   <WPAC_version>1.0</WPAC_version>
   <WPAC_gatewayID>http://wpas_wsp_gateway_uri</WPAC_gatewayID>
   <WPAC_identifier>000000B7</WPAC_identifier>
   <WPAC_sent>2015-02-25T14:55:00-07:00</WPAC_sent>
   <WPAC_status>System</WPAC_status>
   <WPAC_msgType>Transmission Control - Resume</WPAC_msgType>
</WPAC_attributes>
```

8.6 Transport Protocol

Transmission Control Protocol (TCP) [Ref 17] is the transport protocol used to transmit WPAC messages and manage overall transmission control between the NAADS WPA Gateway and the WSP Gateway on the C-Interface.

Transmission Control Protocol (TCP) and Internet Protocol (IP) shall be implemented as detailed in the following requirements. Each NAADS WPA Gateway to WSP Gateway connection shall be defined by a unique socket pair, consisting of the source IP address, source port number, destination IP address, and destination port number, where the source and destination IP addresses are obtained from the IP address or Fully Qualified Domain Name contained in the WSP profile and NAADS WPA Gateway profile.

1. [WPA-C-RQMT-3000] The NAADS WPA Gateway to WSP Gateway interface shall be in accordance with RFC 1122 [Ref 18].

8.6.1 Transmission Control Protocol (TCP)

TCP shall be the transport level protocol used by the NAADS WPA Gateway and the WSP Gateway to exchange messages. TCP is a connection-oriented protocol and thus requires establishment of a connection to another system to facilitate data transfer. The interface shall use persistent connections. A Gateway shall close a connection only after providing notification to the other Gateway.

1. [WPA-C-RQMT-3100] Transmission Control Protocol (TCP) shall be implemented for the transport layer in accordance with RFC 793 [Ref 17].
2. [WPA-C-RQMT-3110] TCP connections shall be persistent.

8.6.2 Internet Protocol (IP)

IP shall be the network layer protocol used by the NAADS WPA Gateway and the WSP Gateway to exchange WPAC messages. It is requested that IP Version 6 (IPv6) be employed wherever possible. Where there may be technical constraints, IPv4 may be optionally used on an as needed basis by a WSP and the NAAD System.

1. [WPA-C-RQMT-3220] It is recommended that the interface shall support IP Version 6 for the network layer in accordance with RFC 2460 [Ref 21], RFC 2464 [Ref 22], RFC 4291 [Ref 23], and RFC 4443 [Ref 24].
2. [WPA-C-RQMT-3200] Where necessary, the interface shall optionally support IP Version 4 for the network layer in accordance with IETF STD 5 (RFC 791) [Ref 19].
3. [WPA-C-RQMT-3210] Where necessary, the network layer shall optionally support Internet Control Message Protocol (ICMP) in accordance with IETF STD 5 (RFC 792) for IP Version 4 [Ref 20].

8.7 Error Handling

8.7.1 TCP/IP Error Handling

This interface uses the reliable TCP protocol to correct any transmission errors that occur at IP or lower layers. Using TCP isolates such errors from HTTP and WPAC protocol layers. TCP uses a retransmission mechanism to correct any errors in received packets.

1. [WPA-C-RQMT-3300] Any packets received in error shall be discarded at TCP level by the receiving gateway.
2. [WPA-C-RQMT-3310] When a packet is received in error, a correct packet shall be retransmitted by the sending gateway per TCP protocol.
3. [WPA-C-RQMT-3320] Both the WSP Gateway and the NAADS WPA Gateway shall log failures to establish a TCP session.
4. [WPA-C-RQMT-3330] Both the WSP Gateway and the NAADS WPA Gateway shall log failures to establish a secure IP tunnel.

8.7.2 HTTP Level Error Handling

As only HTTP POST methods shall be used on this interface, all other HTTP methods are to be rejected.

1. [WPA-C-RQMT-3400] The NAADS WPA Gateway shall reject all HTTP methods other than POST with a 4xx Client Error response when the WSP Gateway sends a WPAC message.
2. [WPA-C-RQMT-3410] The WSP Gateway shall reject all HTTP methods other than POST with a 4xx Client Error response.

8.7.3 WPAC Error Handling

8.7.3.1 Schema Validation

1. [WPA-C-RQMT-3500] Messages not conforming to the WPAC schema shall be logged and discarded.

NOTE: See Section 7.4, *WPAC Message XML Definition*, for the WPAC schema.

2. [WPA-C-RQMT-3510] An Error message shall be sent in response to messages not conforming to the WPAC schema.

8.7.3.2 WPAC Message Content Validation

The format of each WPAC message is detailed as follows:

- Alert (*Section 8.5.1, Alert Message*)
- Update (*Section 8.5.2, Update Message*)
- Cancel (*Section 8.5.3, Cancel Message*)
- WPAS Test (*Section 8.5.7, WPA System Test Message*)
- Link Test (*Section 8.5.6, Link Test Message*)
- Ack (*Section 8.5.4, Ack Message*)
- Error (*Section 8.5.5, Error Message*)
- Transmission Control – Cease (*Section 8.5.8, Transmission Control – Cease Message*)
- Transmission Control – Resume (*Section 8.5.9, Transmission Control – Resume Message*)

1. [WPA-C-RQMT-3600] Messages containing information that conflicts with the WPAC protocol shall be logged and discarded.
2. [WPA-C-RQMT-3610] An Error message shall be sent in response to messages containing information that conflicts with the WPAC protocol. See *Table 32: Definition of WPAC Response Codes,* for error response codes.

8.7.3.3 Error Response Codes

Error response codes (see *Table 32: Definition of WPAC Response Codes*) are used by the NAADS WPA Gateway and the WSP Gateway in Error messages only. Though Ack and Error messages may contain errors, the response codes would not be used as those errors shall not be reported in Error messages.

Each Error message shall contain one or more of the response codes listed in *Table 32: Definition of WPAC Response Codes.*

The following table defines the response codes and the response description that may be returned in the WPAC_responseCode and WPAC_note elements in response to a received WPAC message via the C-Interface. In addition, the following table defines the associated message types for the response codes and provides any explanatory notes.

Table 32: Definition of WPAC Response Codes

RESPONSE CODE	RESPONSE DESCRIPTION INCLUDED IN WPAC_NOTE ELEMENT	ASSOCIATED MESSAGE TYPE	NOTES
100	invalid-naad-system-wpas-alert-gateway-id	Error	The sending gateway identifier is not valid.
101	protocol–version-not-supported	Error	The gateway does not support the indicated protocol version.
102	server-error	Error	General error in the server.
103	invalid-format	Error	The received XML has an invalid format.
104	invalid-element XXX	Error	XXX replaced with the name of the invalid element.
105	missing-element XXX	Error	XXX replaced with name of missing element.
106	operation-not-allowed	Error	The requested operation is not allowed.
107	operation-pre-empted	Error	The requested operation (e.g., a WPAS TEST) was pre-empted and not completed.
108	wpas-test- distribution-precluded	Error	Unforeseen condition in WSP infrastructure precludes distribution of WPA System Test information.

ANNEX B CONFIGURABLE PARAMETERS

This annex defines the configurable parameters that are associated with the C-Interface. The WSP Profile and the NAADS WPA Gateway Profile contain configurable parameters, as defined in Table 3 and Table 4 respectively.

The following table identifies additional configurable parameters, describes their usage, and identifies the maximum parameter range.

Table 33: Configurable Parameters

PARAMETER NAME	PARAMETER DESCRIPTION	PARAMETER SETTING
Message Response Time	The period of time in which NAADS WPA Gateway or WSP Gateway expects to receive a response from one another.	1 to 10 seconds.
WSP Gateway Maximum Messages	Maximum Number of Alert, Update, Cancel Messages or WPA System Test Messages that can be processed by the WSP Gateway in a single minute.	20 - 30 Note: The WSP Gateway has the ability to buffer and queue messages should there be a backlog in the CBC or LTE Network.
NAADS WPA Gateway Retransmit Number	The number of times that the NAADS WPA Gateway shall attempt to send a WPAM to the WSP Gateway when the expected response is not received.	1 to 10.
WSP Gateway Retransmit Number	The number of times that the WSP Gateway shall attempt to send a Link Test, Transmission Control – Cease, Transmission Control - Resume to the NAADS WPA Gateway when the expected response is not received.	1 to 10.
NAADS WPA Gateway Link Test Periodicity	The time interval between Link Test Messages as transmitted by the NAADS WPA Gateway to the WSP Gateway.	1 - 15 Minutes as determined by the NAAD System and the respective WSP.
WSP Gateway Link Test Periodicity	The time interval between Link Test Messages as transmitted by the WSP Gateway to the NAADS WPA Gateway to the WSP Gateway.	As Required.
Minimum Character Length	Minimum number of bilingual French/English Characters that are to be processed by the by the WSP Gateway (within the Cell Broadcast System). If below this value, processing of the WPAM may be rejected and an appropriate corresponding Error Message shall be returned to the NAADs WPA Gateway.	1 (WPAMs must contain at least 1 Character)
Minimum and Maximum Character Length	Maximum number of bilingual French/English Characters that are to be processed by the by the WSP Gateway (within the Cell Broadcast System). If above this value, processing of the WPAM may be rejected and an appropriate corresponding Error Message shall be returned to the NAADs WPA Gateway.	600 in accordance with the National Public Alerting System Common Look and Feel Guidance [Ref 32]

PARAMETER NAME	PARAMETER DESCRIPTION	PARAMETER SETTING
Maximum Upset Expiry for an Alert, Update or WPA System Test Message.	The highest expiry value permitted by the WSP Gateway (within the Cell Broadcast System). If above this value, processing of the WPAM may be rejected and an appropriate corresponding Error Message shall be returned to the NAADs WPA Gateway.	24 Hours

ANNEX C NPAS PUBLIC AWARENESS TESTS – WPA CONSIDERATIONS

NPAS Public Awareness Tests are generated in accordance with SOREM Testing Policies and they contain text fields that explicitly explain to a mobile phone subscriber that they are test messages only. For WPA, the WPA Mandatory Reception Channel (MI=4370) will be used once per year during Emergency Preparedness Week in May in accordance with Telecom Regulatory Policy CRTC 2017-91 [Ref 42]. For all other such tests throughout the year, the NPAS Public Awareness Test Messages will be delivered over the WPA System Test Channel (MI=4380).

The policy pertaining to which WPA channel is used for NPAS Public Awareness Tests is beyond the scope of this specification. Furthermore, the mechanism through which Alert Issuers will route an NPAS Public Awareness Test Message to either the WPA Mandatory Reception Channel (MI=4370) or the WPA System Test Channel (MI=4380) is upstream of the WPA C-Interface and therefore beyond he scope of this specification.