

HITSP Emergency Common Alerting Protocol Component

HITSP/C82



Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

**Security, Privacy, and Infrastructure Domain Technical Committee
(Formerly Security and Privacy Technical Committee)**



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
	Template Updated to V2.4	Project Team	August 31, 2008
0.0.1	Review Copy	Security, Privacy, and Infrastructure Domain Technical Committee	September 26, 2008
0.0.2	Review Copy	Security, Privacy, and Infrastructure Domain Technical Committee	December 10, 2008
1.0	Released for Implementation	Security, Privacy, and Infrastructure Domain Technical Committee	December 18, 2008
	Template V2.5	Project Team	June 30, 2009
1.0.1	Review Copy	Security, Privacy, and Infrastructure Domain Technical Committee	June 30, 2009
1.1	Released for Implementation	Security, Privacy, and Infrastructure Domain Technical Committee	July 8, 2009



TABLE OF CONTENTS

1.0	INTRODUCTION	5
1.1	Overview	5
1.2	Copyright Permissions	5
1.3	Reference Documents	5
1.4	Conformance	5
1.4.1	Conformance Criteria	5
1.4.2	Conformance Scoping, Subsetting and Options	6
2.0	COMPONENT DEFINITION	7
2.1	Context Overview	7
2.1.1	Component Constraints	7
2.1.2	Component Dependencies	7
2.2	Rules for Implementing	7
2.2.1	Data Mapping	8
2.3	Standards	8
2.3.1	Regulatory Guidance	8
2.3.2	Selected Standards	8
2.3.3	Informative Reference Standards	8
3.0	APPENDIX	9
4.0	DOCUMENT UPDATES	10
4.1	December 10, 2008	10
4.2	December 18, 2008	10
4.3	June 30, 2009	10
4.4	July 8, 2009	10



FIGURES AND TABLES

Table 1-1 Reference Documents	5
Table 2-1 Component Constraints	7
Table 2-2 Component Dependencies	7
Table 2-3 Data Mapping	8
Table 2-4 Regulatory Guidance	8
Table 2-5 Selected Standards	8
Table 2-6 Informative Reference Standards	8



1.0 INTRODUCTION

1.1 OVERVIEW

The HITSP Emergency Common Alerting Protocol Component is based on the Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol (CAP) v1.1 standard, and is used as a multicast notification message sent to an identified channel. The intended recipients are populations such as “all emergency departments in XXX county”, “within a geographic area”, etc.

1.2 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2009 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI's copyright is clearly noted.

OASIS materials used in this document have been extracted from relevant copyrighted materials with permission of the Organization for the Advancement of Structured Information Standards (OASIS). Copies of this standard are available from OASIS at www.oasis-open.org.

1.3 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material.

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from www.hitsp.org.

Table 1-1 Reference Documents

Reference Document	Document Description
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
TN900 - Security and Privacy	TN900 is a reference document to provide the overall context for use of the HITSP Security and Privacy constructs

1.4 CONFORMANCE

This section describes the conformance criteria, which are objective statements of requirements that can be used to determine if a specific behavior, function, interface, or code set has been implemented correctly.

1.4.1 CONFORMANCE CRITERIA

In order to claim conformance to this construct specification, an implementation must satisfy all the requirements and mandatory statements listed in this specification, the associated HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must also implement all of the required interfaces within the scope, subset or implementation option that is selected from the associated Interoperability Specification.

Claims of conformance may only be made for the overall HITSP Interoperability Specification or Capability with which this construct is associated.



1.4.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification must be implemented in its entirety for an implementation to claim conformance to the specification. HITSP may define the permissibility for interface(s) scoping, subsetting or implementation options by which the specification may be implemented in a limited manner. Such scoping, subsetting and options may extend to associated constructs, such as this construct. This construct must implement all requirements within the selected scope, subset or options as defined in the associated Interoperability Specification to claim conformance.



2.0 COMPONENT DEFINITION

2.1 CONTEXT OVERVIEW

The purpose of this Component is to specify a multicast notification message which is sent to an identified channel. The intended recipients are populations such as “all emergency departments in XXX County.” This construct can only be used to transport text message alerts.

This construct is based on the Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol (CAP) v1.1 standard.

The text for the OASIS Common Alerting Protocol (CAP) v1.1 specification begins here:

A simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

The text for the OASIS Common Alerting Protocol (CAP) v1.1 specification ends here.

OASIS CAP is intended to be used in a point to point conversation between Distribution Elements. The existing HITSP Security and Privacy protections can be applied. HITSP/TN900 Security and Privacy provides guidance on how to ensure privacy through appropriate security mechanisms.

The system from the related Interoperability Specification that implements the Distribution Element may use multicast methods (e.g., pager, radio, and email) to ultimately communicate with the end systems.

2.1.1 COMPONENT CONSTRAINTS

Table 2-1 Component Constraints

Constraint	Constraint Section
No applicable constraints	

2.1.2 COMPONENT DEPENDENCIES

Table 2-2 Component Dependencies

Standard/HITSP Component	Depends On (Name of standard/HITSP Component that it depends on)	Dependency Type (Pre-condition, Post-condition, General)	Purpose (Reason for this dependency)
No applicable dependencies			

2.2 RULES FOR IMPLEMENTING

This document is a component construct instead and does not specify transactions. The reason for this is that future versions of OASIS CAP will be transported by HITSP/T63 Emergency Message Distribution Element, and will no longer be a communications protocol. OASIS DE will become the new communication protocol for OASIS CAP. OASIS CAP can be used as a communications protocol by itself, as is done in many existing implementations. However, it is recommended that future implementations focus on the use of OASIS CAP being transported by HITSP/T63, which uses OASIS EDXL-DE. Detailed specifications are provided in the OASIS CAP v1.1 October 2005 specification.



2.2.1 DATA MAPPING

The Interoperability Specification that uses this construct may impose restrictions on the CAP data content. However, this construct does not impose any restrictions at this time.

Examples of OASIS CAP content may be found in the OASIS CAP standard.

Table 2-3 Data Mapping

Data Element	Description	Limit/Range of values	Data Source	Destination	Requirements/Pre-conditions	Additional Specification for Component
No applicable data mapping						

2.3 STANDARDS

2.3.1 REGULATORY GUIDANCE

Table 2-4 Regulatory Guidance

Regulation	Description
No applicable regulatory guidance	

2.3.2 SELECTED STANDARDS

Table 2-5 Selected Standards

Standard	Description
Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol (CAP) V1.1, October 2005	This is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience. For more information visit www.oasis-open.org

2.3.3 INFORMATIVE REFERENCE STANDARDS

Table 2-6 Informative Reference Standards

Standard	Description
No applicable informative reference standards	



3.0 APPENDIX

The following sections include relevant materials referenced throughout this document.

No additional information at this time.



4.0 DOCUMENT UPDATES

The following sections provide the details of updates made to this document.

4.1 DECEMBER 10, 2008

The changes in this construct address the following comments received during the Public Comment and Inspection Testing period (September 29 – October 24, 2008).

No comments were received.

Minor editorial changes were made to this document.

4.2 DECEMBER 18, 2008

Upon approval by the HITSP Panel on December 18, 2008, this document is now Released for Implementation.

4.3 JUNE 30, 2009

Minor editorial changes were made to this document. Boilerplate text was removed for simplification. The term “actor” was replaced with the term “interface”.

4.4 JULY 8, 2009

Upon approval by the HITSP Panel on July 8, 2009, this document is now Released for Implementation.

