



**Satellite Earth Stations and Systems (SES);
Satellite Emergency Communications;
Multiple Alert Message Encapsulation over Satellite (MAMES)**

Reference

DTS/SES-00310

Keywords

emergency, satellite

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	7
Foreword.....	7
Modal verbs terminology.....	7
1 Scope	8
2 References	8
2.1 Normative references	8
2.2 Informative references.....	8
3 Definitions and abbreviations.....	9
3.1 Definitions.....	9
3.2 Abbreviations	12
4 MAMES Objectives and Operation	13
4.1 MAMES Objectives	13
4.2 Overview of MAMES Operation	13
4.2.1 MAMES Network Entities: MAMES Provider and MAMES Receiver	13
4.2.2 MAMES Operative Modes: Direct and Indirect MAMES Alerting	14
4.2.3 The MAMES Agents	15
4.2.3.1 MAMES Network Reference Model.....	15
4.2.3.2 MAMES Alerter-Side Agent.....	16
4.2.3.3 MAMES User-Side Agent	16
5 MAMES Architecture	16
5.1 Functional Architecture	16
5.2 Protocol Architecture	17
5.2.1 MAMES Positioning in a Protocol-stack Architecture	17
5.2.2 Protocol Architecture for Direct MAMES Alerting.....	19
5.2.2.1 Scenario A1	19
5.2.2.2 Scenario A2.....	20
5.2.3 Protocol Architecture for Indirect MAMES Alerting	21
5.2.3.1 Scenario B1	21
5.2.3.2 Scenario B2.....	22
6 MAMES Messages.....	23
6.1 Overall Structure	23
6.2 MAMES Message Types.....	24
6.2.1 Overview of MAMES Message Types	24
6.2.2 MAMES ALERT	25
6.2.3 MAMES Ultra-Short ALERT.....	26
6.2.4 MAMES UPDATE	26
6.2.5 MAMES CANCEL.....	27
6.2.6 MAMES ACK	27
6.3 MAMES Message Headers	28
6.3.1 MAMES Mandatory Headers	28
6.3.1.1 General Features	28
6.3.1.2 The ALERT Mandatory Header.....	28
6.3.1.3 The Ultra-Short ALERT Mandatory Header.....	28
6.3.1.4 The UPDATE Mandatory Header.....	29
6.3.1.5 The CANCEL Mandatory Header.....	29
6.3.1.6 The ACK Mandatory Header	29
6.3.2 MAMES Extension Headers.....	29
6.3.2.1 General Features	29
6.3.2.2 Alert and Response Type Header.....	30
6.3.2.3 Incident Header	30
6.3.2.4 Validity Header	30
6.3.2.5 Administrative Areas Header	31
6.3.2.6 Authentication/Integrity Header.....	31
6.3.2.7 Encryption Header	31

6.3.3	The Alert Message Header.....	32
6.3.4	MAMES Headers Concatenation Algorithm	32
6.4	MAMES Header Fields	33
6.4.1	Fields of Mandatory Headers.....	33
6.4.1.1	MAMES Protocol Version.....	33
6.4.1.2	MAMES Message Type.....	33
6.4.1.3	MAMES Message ID.....	33
6.4.1.4	MAMES Alert Provider ID.....	34
6.4.1.5	Notification Area.....	34
6.4.1.6	MAMES Transport Priority	34
6.4.1.7	ACK Request Indicator	34
6.4.1.8	Alert Issuer ID.....	35
6.4.1.9	Next Header Type	35
6.4.1.10	MAMES Reference	35
6.4.1.11	MAMES Receiver Location.....	36
6.4.1.12	MAMES Receiver ID.....	36
6.4.2	Fields of Alert and Response Type Header	36
6.4.2.1	MAMES Status	36
6.4.2.2	MAMES Alert Scope	37
6.4.2.3	MAMES Response Type.....	37
6.4.2.4	MAMES Event Category	38
6.4.3	Fields of Incident Header.....	38
6.4.3.1	MAMES Incident ID.....	38
6.4.3.2	Issuance Time	39
6.4.4	Fields of the Validity Header	39
6.4.4.1	MAMES Validity Start	39
6.4.4.2	MAMES Validity End.....	39
6.4.5	Fields of the Administrative Areas Header.....	40
6.4.5.1	Administrative Areas Header Version	40
6.4.5.2	Administrative Areas Coding.....	40
6.4.5.3	Number of Areas	40
6.4.5.4	Area IDs	40
6.4.6	Fields of the Authentication/Integrity Header	41
6.4.6.1	Authentication/Integrity Header Version	41
6.4.6.2	Authentication/Integrity Flag	41
6.4.6.3	Authentication/Integrity Algorithm ID	41
6.4.6.4	MAC Value Length.....	41
6.4.6.5	MAC Value	42
6.4.7	Fields of the Encryption Header	42
6.4.7.1	Encryption Header Version.....	42
6.4.7.2	Encryption Algorithm ID	42
6.4.7.3	Initialization Vector Length	42
6.4.7.4	Initialization Vector	42
6.4.7.5	Block Size	43
6.4.7.6	Number of Padding Bytes	43
6.4.8	Fields of the Alert Message Header.....	43
6.4.8.1	Alert Message Type	43
6.4.8.2	Language ID.....	44
6.4.8.3	Alert Message Length	44
6.4.8.4	More AMHs Flag	44
7	Behaviour of MAMES Agents	44
7.1	Identification of a Set of behaviours.....	44
7.2	MAMES Alert Provider Actions	45
7.2.1	Actions of MAMES Provider upon reception of an Alert Message from Alert Issuer (MAMES Composition Process)	45
7.2.2	Actions of MAMES Provider for declaring a previous transmitted MAMES Frame obsolete (MAMES Composition Process)	46
7.2.3	Actions of MAMES Provider upon reception of a MAMES ACK from MAMES Receiver (ACK Parsing Process).....	47
7.3	MAMES Alert Receiver Actions.....	47

7.3.1	Actions of MAMES Receiver upon reception of a MAMES Frame (Parsing Process and MAMES ACK Composition Process).....	47
7.3.2	Actions of MAMES Receiver upon reception of an Alert acknowledgement from an Alerting Device (MAMES ACK Composition Process).....	49
Annex A (normative): MAMES Requirements.....		50
A.1	General Functional Requirements	50
A.2	MAMES Alerter-Side Agent Requirements.....	50
A.3	MAMES User-Side Agent Requirements	51
Annex B (normative): MAMES Frame Field Details		52
B.1	Mandatory Header Fields Details.....	52
B.1.1	Notification Area Field Details	52
B.2	Extension Header Fields Details	52
B.2.1	<Area IDs>: Administrative Area Codes Mapping.....	52
B.3	Alert Message Header Fields Details	53
B.3.1	<Language ID> Codes	53
B.3.2	<Alert Message Type>: Internet Media Type Mapping.....	56
Annex C (informative): MAMES Frames Examples.....		58
C.1	MAMES ALERT Frame	58
C.2	MAMES Ultra-short ALERT Frame.....	59
C.3	MAMES UPDATE Frame	59
C.4	MAMES CANCEL Frame	59
C.5	MAMES ACK Frame.....	60
Annex D (normative): MAMES Headers Concatenation.....		61
D.1	Adopted Notation: Headers Fields Numbering	61
D.2	Mandatory Headers Fields Positioning	62
D.2.1	General Features.....	62
D.2.2	ALERT MH.....	62
D.2.3	Ultra-Short ALERT MH	62
D.2.4	UPDATE MH.....	63
D.2.5	CANCEL MH	63
D.2.6	ACK MH.....	63
D.3	Extension Headers <i>non-rotated</i> and <i>rotated</i> Versions.....	63
D.3.1	General Features.....	63
D.3.2	Alert and Response Type Header	64
D.3.3	Incident Header	64
D.3.4	Validity Header	65
D.3.5	Administrative Areas Header	65
D.3.6	Authentication/Integrity Header	66
D.3.7	Encryption Header.....	66
D.4	Alert Message Header <i>Non-rotated</i> and <i>Rotated</i> Versions	67
Annex E (informative): Description of the Behaviour of the MAMES Agents.....		68
E.1	Adopted Notation	68
E.2	MAMES System and MAMES Blocks	69
E.3	MAMES Processes.....	70
E.3.1	Overview of the MAMES Processes and Corresponding Procedures	70
E.3.2	MAMES Alerter-Side Agent Processes	71

E.3.3 MAMES User-Side Agent Processes73
History75

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document establishes the specifications for the MAMES (Multiple Alert Message Encapsulation over Satellite) Protocol. Starting from an overview of the MAMES objectives and operations, the MAMES Architecture is presented: the MAMES functional entities are identified and the MAMES positioning in a protocol-stack architecture is provided by defining a set of MAMES operational scenarios.

The MAMES alert message encapsulation scheme is specified by defining the overall MAMES Message structure, the different types of MAMES messages and all MAMES Header fields.

The behaviour of the MAMES Agents responsible for the process of the MAMES Protocol is defined.

Guidelines for integrating the MAMES alert message encapsulation scheme into communications networks are provided in [i.1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

- [1] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".
- [2] IETF RFC 4868: "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec".
- [3] IETF RFC 4493: "The AES-CMAC Algorithm".
- [4] IETF RFC 4494: "The AES-CMAC-96 Algorithm and Its Use with IPsec".
- [5] IETF RFC 3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec".
- [6] IETF RFC 3686: "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)".
- [7] Recommendation ITU-T X.1303: "Common alerting protocol (CAP 1.1)".
- [8] OASIS Standard: "Common Alerting Protocol Version 1.2".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI TR 103 338: "Satellite Earth Stations and Systems (SES); Satellite Emergency Communications (SatEC); Multiple Alert Message Encapsulation over Satellite (MAMES) deployment guidelines".

[i.2] ISO/IEC 27000:2014: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

[i.3] <http://csrc.nist.gov/groups/ST/toolkit/index.html>.

[i.4] NUTS (Nomenclature of Territorial Units for Statistics), by regional level, version 2010 (NUTS 2010).

NOTE: Available at:

http://ec.europa.eu/eurostat/ramon/nomenclatures/index.cfm?TargetUrl=LST_CLS_DLD&StrNom=NUTS_33&StrLanguageCode=EN.

[i.5] NUTS - Nomenclature of territorial units for statistics, Local Administrative Units (LAU).

NOTE: Available at: <http://ec.europa.eu/eurostat/web/nuts/local-administrative-units>.

[i.6] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

[i.7] "Communication system for the dissemination of alert messages: Architecture and design document", Deliverable D3.6, Alert for All (A4A) project.

[i.8] ISO 639-1:2002: "Codes for the representation of names of languages -- Part 1: Alpha-2 code".

[i.9] Media Types.

NOTE: Available at <http://www.iana.org/assignments/media-types/media-types.xhtml>.

[i.10] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.11] European Commission Mandate M/496 (2011): "Mandate Addressed to CEN, CENELEC and ETSI to Develop Standardization Regarding Space Industry (Phase 3 of the Process)".

[i.12] L. Franck, R. Suffritti, "Multiple Alert Message Encapsulation over Satellite", 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009, Wireless VITAE 2009, May 2009.

[i.13] ETSI TS 102 182: "Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies".

[i.14] ETSI TS 102 900: "Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service".

[i.15] ETSI TS 122 268: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Public Warning System (PWS) requirements (3GPP TS 22.268 version 12.2.0 Release 12)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Alert Intermediary System: telecommunications network or node that is located at the user side of the Alert Network and that forwards alert-related (MAMES or non-MAMES) messages

Alert Issuer: entity that generates Alert Messages and forwards them to a MAMES Alert Provider for MAMES Encapsulation; more generally, entity that terminates an Alert Protocol at the alerter side of an Alert Network

NOTE: Depending on the Alert Protocol used, an Alert Issuer may be capable of updating or cancelling a previously issued Alert Message, and of requesting and accepting acknowledgement messages.

Alert Message: Alert Protocol Message containing data to alert and/or inform Alert Users about an impending or on-going emergency

Alert Network: in the context of the present document, telecommunications or navigation network that supports Alert Protocol Messages

Alert Protocol: protocol used to exchange Alert Protocol Messages

NOTE 1: In its most basic form, an Alert Protocol is a simple, mutually agreed rule for encoding alert-related information (e.g. by specifying an Internet media type).

NOTE 2: An advanced Alert Protocol typically includes, in addition to an Alert Message, other specially formatted messages for the purpose of updating, cancelling or acknowledging a previous Alert Protocol Message. An example of an advanced Alert Protocol is CAP.

NOTE 3: The termination points of an Alert Protocol are the Alert Issuer (at the alerter side) and the Alerting Device or the Mediation Device (at the user side).

Alert Protocol Message: message conforming to an Alert Protocol

NOTE: The term Alert Protocol Message comprises messages designed to alert or update Alert Users, as well as messages designed to cancel or acknowledge a previously transmitted Alert Protocol Message.

Alert User: entity that consumes the rendered content of an Alert Protocol Message

NOTE 1: A typical Alert User is a physical person that (e.g.) reads an Alert Message text on a display; an Alert User may also be a technical system that is triggered by the contents of an Alert Message to perform certain tasks (e.g. close a floodgate).

NOTE 2: Alerting Devices are not considered to be Alert Users, since they do not consume, but in fact render the contents of Alert Messages.

Alerting Device: device that receives an Alert (Protocol) Message and renders its content to one or more Alert User(s) according to its rendering capabilities; more generally, entity that terminates an Alert Protocol at the user side of an Alert Network

NOTE 1: Depending on the Alert Protocol used, an Alerting Device may be capable of returning acknowledgement messages.

NOTE 2: An Alerting Device contains one or more Alerting Function(s) and it may contain one or more Mediation Function(s).

NOTE 3: An example of an Alerting Device is a siren that activates the proper tone for alerting the population; another example is a smartphone that displays the Alert Message content.

Alerting Function: logical function within an Alerting Device that receives the alert indication or information and renders these data according to its capabilities

Alerting Services Regulator: authority that regulates the implementation and provision of alerting services within its area of authority

CAP Capable Device: Alerting Device or Mediation Device that is capable of processing a CAP-compliant Alert Protocol Message; more generally, device that terminates the CAP protocol at the user side of a CAP-based Alert Network

Direct MAMES Alerting: MAMES-based alerting scheme whereby the Satellite Terminal and the MAMES Receiver are co-located, i.e. either integrated into a single device or interconnected via a direct physical link

Indirect MAMES Alerting: MAMES-based alerting scheme whereby the Satellite Terminal and the MAMES Receiver are interconnected via a network, referred to as an Alert Intermediary System

MAMES Agent: software module that executes the MAMES Protocol

NOTE: Two types of MAMES Agents exist: The MAMES Alerter-Side Agent and the MAMES User-Side Agent.

MAMES Alert Provider: entity that generates MAMES Messages; more generally, entity that terminates the MAMES Protocol at the alerter side of a MAMES Network

NOTE: A MAMES Alert Provider is also capable of requesting and accepting MAMES-based acknowledgement (ACK) messages.

MAMES Alert Receiver: entity that is capable of receiving MAMES Messages; more generally, entity that terminates the MAMES Protocol at the user side of a MAMES Network

NOTE: A MAMES Alert Receiver is also capable of generating MAMES-based acknowledgement (ACK) messages.

MAMES Alerter-Side Agent: MAMES Agent serving the MAMES Alert Provider

MAMES Alerter-Side Controller: entity within the MAMES Alert Provider that configures, monitors and controls a MAMES Alerter-Side Agent

NOTE: The MAMES Alerter-Side Controller may be a software module operated by a physical person in charge of initiating and configuring a MAMES Alerter-Side Agent, and of controlling its operation in coordination with the Alert Issuer; alternatively, it may be an autonomous software algorithm performing these tasks.

MAMES Decapsulation: process of decapsulating a MAMES Frame to obtain the message(s) contained in the MAMES Payload

NOTE: Both the MAMES User-Side Agent and the MAMES Alerter-Side Agent are capable of MAMES Decapsulation.

MAMES Encapsulation: process of encapsulating one or more Alert Protocol Message(s) into a MAMES Frame

NOTE: Both the MAMES Alerter-Side Agent and the MAMES User-Side Agent are capable of MAMES Encapsulation.

MAMES Frame: used interchangeably with the term MAMES Message

MAMES Governing Body: authority that governs and regulates the operations and communications of all MAMES entities

MAMES Message: message conforming to the MAMES format

NOTE: MAMES Messages consist of a MAMES Header and (optionally) a MAMES Payload.

MAMES Network: Alert Network that supports the distribution and exchange of MAMES Messages

MAMES Payload: Alert Protocol Message(s) contained within a MAMES Frame

MAMES Protocol: Alert Protocol that supports the distribution and exchange of MAMES Messages

MAMES Provider: used interchangeably with the term MAMES Alert Provider

MAMES Receiver: used interchangeably with the term MAMES Alert Receiver

MAMES User-Side Agent: MAMES Agent serving the MAMES Alert Receiver

MAMES User-Side Controller: entity within the MAMES Alert Receiver that configures, monitors and controls a MAMES User-Side Agent

NOTE: Once initiated, the MAMES User-Side Controller is an autonomously running software algorithm.

Mediation Device: device hosting one or more Mediation Function(s)

Mediation Function: in the context of the present document, logical function that performs a protocol conversion between two different Alert Protocols

NOTE 1: A Mediation Function is required in cases when the Alerting Device (e.g. a siren) is not capable of processing the incoming Alert Message (e.g. a CAP message).

NOTE 2: A Mediation Function may be implemented as a stand-alone device (Mediation Device), or it may be embedded within an Alerting Device.

SatCom/SatNav/Com Network: communications network based on satellite communications, satellite navigation or terrestrial communications (wired, wireless, or mobile) technology

SatCom/SatNav/Com Regulator: authority that regulates the deployment and provision of SatCom/SatNav/Com Networks and services

SatCom/SatNav/Com Service Provider: entity that provides a satellite communications, a satellite navigation or a terrestrial communications service to its subscribers

SatCom/SatNav/Com Subscriber: entity that subscribes to and/or uses a satellite communications, a satellite navigation or a terrestrial communications service offered by a SatCom/SatNav/Com Provider

SatCom/SatNav/Com User Segment: satellite communications, satellite navigation or terrestrial communications subsystem that comprises all SatCom/SatNav/Com network entities at the user side of the SatCom/SatNav/Com Network

SatCom/SatNav Network: communications network based on satellite communications or satellite navigation technology

SatCom/SatNav Ground Segment: satellite communications or satellite navigation subsystem comprising all SatCom/SatNav network entities at the provider side of the SatCom/SatNav Network

SatCom/SatNav Space Segment: communications or navigation satellite(s)

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

A4A	Alert-For-All (Alert4All)
ACK	Acknowledgement
AES	Advanced Encryption Standard
AES-CBC	AES Cipher Block Chaining
AES-CTR	AES Counter
AM	Alert Message
AMH	Alert Message Header
ASN.1	Abstract Syntax Notation One
CAP	Common Alerting Protocol
CBRNE	Chemical, Biological, Radiological, Nuclear or high-yield Explosive threat or attack
CMAC	Cipher-based MAC
EH	Extension Header
EU	European Union
GNSS	Global Navigation Satellite System
HMAC	keyed-Hash Message Authentication Code
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunications Union
JSON	JavaScript Object Notation
LAU	Local Administrative Unit
MAC	Message Authentication Code
MAMES	Multiple Alert Message Encapsulation over Satellite
MB	Megabyte
MH	Mandatory Header
NIST	National Institute of Standards and Technology
NUTS	Nomenclature of Units for Territorial Statistics
OASIS	Organization for the Advancement of Structured Information Standards
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
POCSAG	Post Office Code Standardization Advisory Group
SatCom	Satellite Communication
SatNav	Satellite Navigation

SDU	Service Data Unit
SHA	Secure Hash Algorithm
UTC	Coordinated Universal Time
XML	Extensible Markup Language

4 MAMES Objectives and Operation

4.1 MAMES Objectives

MAMES main objectives are:

- the definition of an encapsulation protocol for Alert Protocol Messages transport over satellite links, as well as over other terrestrial communication links, like GSM, LTE, etc.;
- the provision of a flexible and extensible encapsulation scheme;
- the encapsulation of a single or a concatenation of Alert Protocol Messages (e.g. CAP, unstructured text, image, paging protocols, etc.);
- the definition of additional (optional) functions for service extension and adaption towards specific crisis situations;
- the integration of the defined protocol with the main telecommunication satellite architectures (Galileo Public Regulated Service and Commercial Service data part; DVB-Suite, any IP-based satellite access, etc.) and with terrestrial communication networks.

MAMES is expected to be primarily used over satellite networks, but nothing prevents it to work over other terrestrial networks. The present document focuses on its use for satellite networks.

4.2 Overview of MAMES Operation

4.2.1 MAMES Network Entities: MAMES Provider and MAMES Receiver

The objective of this clause is to provide an overview of MAMES basic operation and introduce the MAMES network entities (MAMES Alert Provider and MAMES Alert Receiver).

Figure 4.1 illustrates the basic MAMES alerting operation, showing the network hierarchy of the alerting chain, the main involved entities, the links between them and exchanged messages.

The aim of Figure 4.1 is to give an overview of the basic MAMES operations and not to provide an exhaustive picture of the applicability of the MAMES protocol in terms of supported types of services.

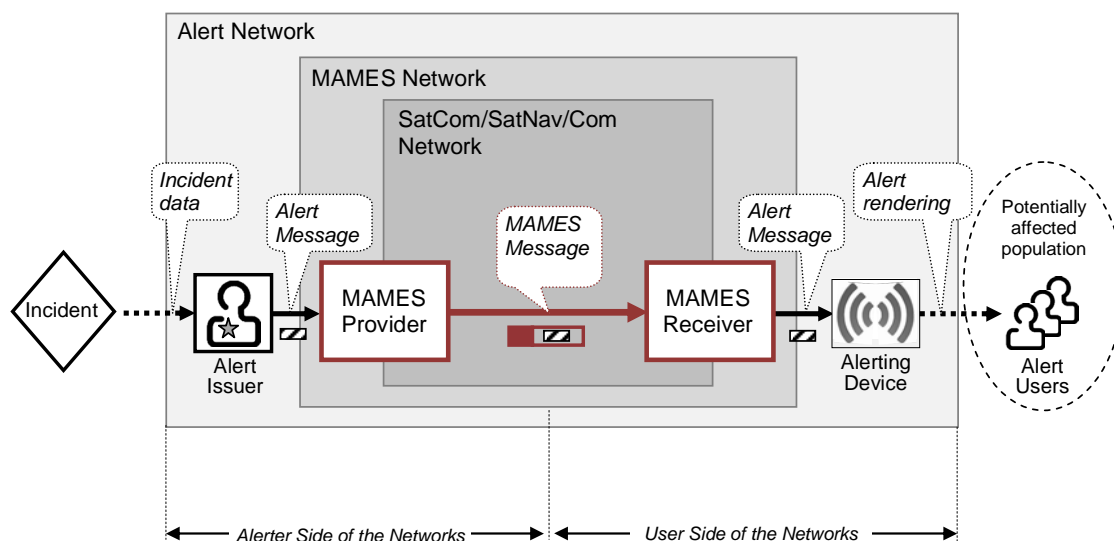


Figure 4.1: Overview of MAMES Operation

In detail the figure depicts only the primary alert flow (forward direction) and no details are shown of the different involved entities.

On the alerter side of the network, upon reception of the relevant collected incident data, the Alert Issuer formulates an Alert Message, which generally carries information on the incident, the population or area to be alerted. The Alert Message is sent to the MAMES Provider, which encapsulates the Alert Message in a MAMES Message and distributes it to the Notification Area, using its connectivity to the SatCom/SatNav/Com Network.

On the user side of the network, upon reception of a MAMES Message, the MAMES Receiver decapsulates the Alert Message, contained in the MAMES payload, after determining (based on location data) whether or not it is allowed to further process the MAMES message. Then the decapsulated Alert Message is forwarded to Alerting Devices, which is in charge of rendering its content to Alert Users.

For the purpose of the present document the focus is on the MAMES network entities responsible for initiating and terminating the MAMES Protocol. These are:

- the MAMES Alert Provider;
- the MAMES Alert Receiver.

Table 4.1 reports the main features of each entity.

Table 4.1: MAMES network entities

MAMES network entity	MAMES network side	Description
MAMES Alert Provider	Alerter side	<p>MAMES network entity that generates MAMES Messages (or MAMES Frames) in the forward link and receives MAMES acknowledgements (if a return link is available):</p> <ul style="list-style-type: none"> • upon reception of an Alert Protocol Message from an Alert Issuer, it is responsible for encapsulating that message in a MAMES Message (forward) and transmitting it via its associated SatCom/SatNav Provider and/or other associated communication provider; • upon reception of a MAMES acknowledgement originated by a MAMES Alert Receiver, it is responsible for handling it.
MAMES Alert Receiver	User side	<p>MAMES network entity that terminates MAMES Protocol and generates MAMES ACKs:</p> <ul style="list-style-type: none"> • upon reception of a MAMES Message originated by a MAMES Alert Provider, it is responsible for decapsulating the Alert Protocol Messages contained in the payload (if any); • upon a request of transmitting an acknowledgement (if a return link is available), it is responsible for generating a MAMES acknowledgement and transmitting it back to the MAMES Alert Provider.

NOTE: The terms MAMES Message and MAMES Frame have exactly the same meaning and can be used interchangeably.

4.2.2 MAMES Operative Modes: Direct and Indirect MAMES Alerting

The two MAMES operative modes are described in the following. Although terrestrial communications networks may also be used to transport MAMES-based messages, in the rest of the document the focus is on the SatCom/SatNav systems.

The two MAMES operative modes are depicted in Figure 4.2. These are:

- *Direct MAMES Alerting.* The MAMES Alert Receiver is inside the satellite user segment and directly receives MAMES Messages; the MAMES Protocol is terminated inside the SatCom/SatNav User Segment.
- *Indirect MAMES Alerting.* The MAMES Alert Receiver is outside the satellite user segment and therefore an intermediary network entity is in charge of forwarding MAMES Messages to the MAMES Alert Receiver; the MAMES Protocol is terminated outside the SatCom/SatNav User Segment.

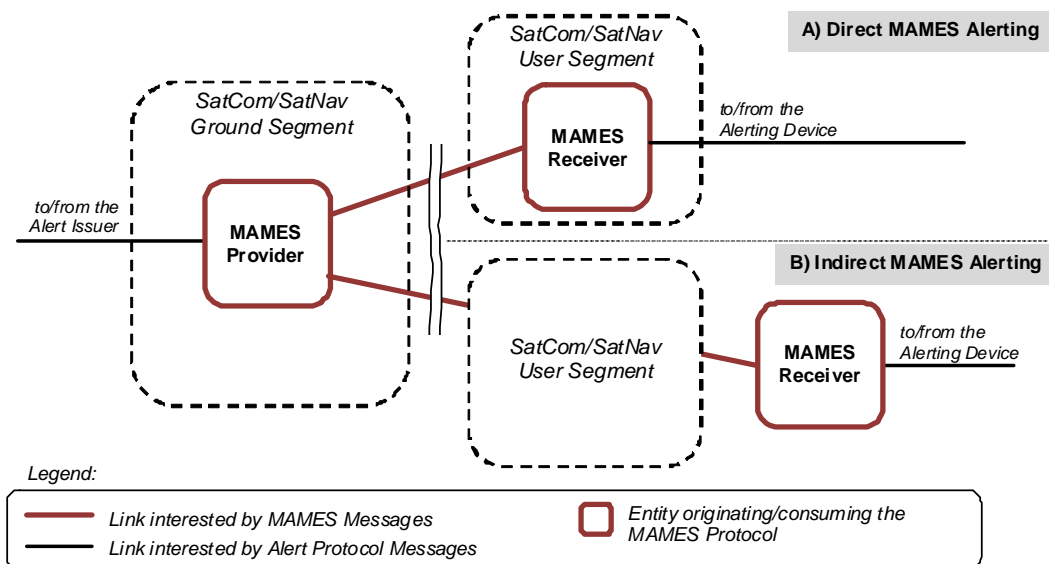


Figure 4.2: MAMES Operative Modes

4.2.3 The MAMES Agents

4.2.3.1 MAMES Network Reference Model

The MAMES protocol service is implemented by MAMES Agents located in the MAMES network entities. A MAMES Agent is a software module that processes the MAMES Protocol. Two types of MAMES Agents are defined:

- the MAMES Alerter-Side Agent;
- the MAMES User-Side Agent.

The former serves the MAMES Alert Provider and the latter the MAMES Alert Receiver.

In Figure 4.3 the MAMES network reference model is depicted. The aim of this figure is to illustrate the MAMES Alerter-Side and User-Side Agents and the interface between them (M), highlighting the main scope of the present document.

Although not addressed in the present document, the interfaces between the MAMES Alerter-Side Agent and the Alert Issuer (I1) and the one between the MAMES User-Side Agent and the Alerting Device (I2) are represented for completeness. However only the behaviour of the MAMES Agents and the communications between them are within the scope of MAMES.

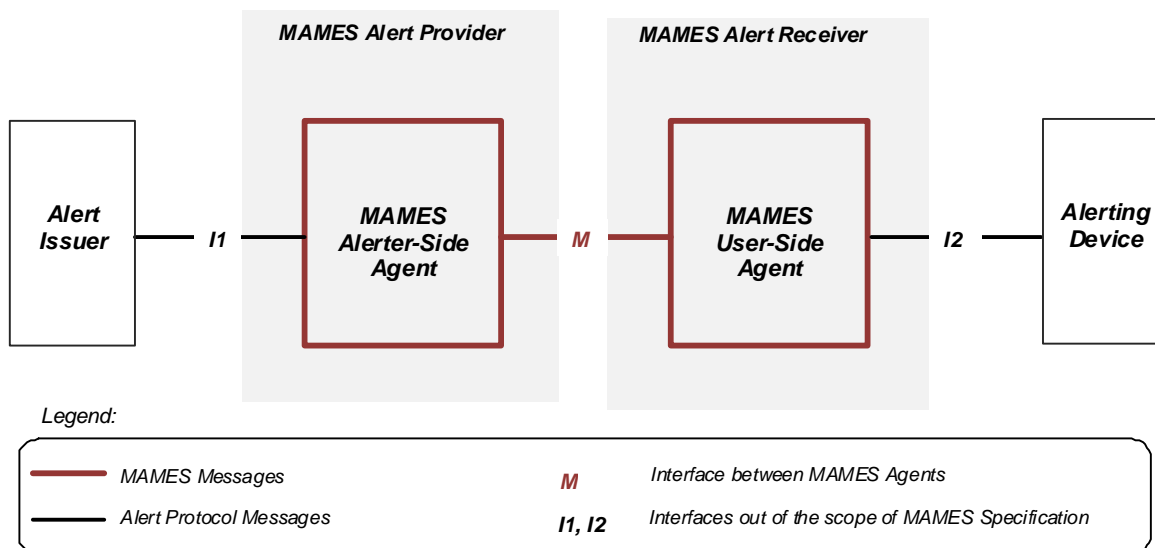


Figure 4.3: MAMES Network Reference Model: MAMES Alerter-Side and User-Side Agents

4.2.3.2 MAMES Alerter-Side Agent

The MAMES Alerter-Side Agent is the MAMES Agent serving the MAMES Alert Provider. It is responsible for the initiation of the MAMES Protocol. Its main function is to receive the Alert Protocol Message as a Service Data Unit (SDU) and produce the MAMES Message as Protocol Data Unit (PDU), enabling the correct transmission of MAMES Message from the MAMES Alert Provider to the MAMES Alert Receiver. Its main functions are:

- composition of MAMES Message, including the encapsulation of Alert Protocol Message(s) (if any) in the payload (*forward link*);
- parsing of MAMES acknowledgement originated by the MAMES Alert Receiver (*return link*), including the decapsulation of the payload of the MAMES acknowledgement, if present.

4.2.3.3 MAMES User-Side Agent

The MAMES User-Side Agent is the MAMES Agent serving the MAMES Alert Receiver. It is responsible for the termination of the MAMES Protocol. Its main functions are:

- parsing of MAMES Message originated by the MAMES Alert Provider, including Alert Protocol Message(s) (if any) decapsulation (*forward link*);
- composition of MAMES acknowledgement including Alert Protocol Message(s) (if any) encapsulation in the payload (*return link*).

5 MAMES Architecture

5.1 Functional Architecture

The objective of this clause is to provide a high level description of the main MAMES functional entities, which shall be part of the MAMES Agents.

A list of the main MAMES functional entities is reported in Table 5.1. For each of them a general description and a specific description based on the MAMES Agents the functional entity belongs to are reported.

In Table 5.1 the terms *primary* and *secondary* functional entity are used with the following meaning. While a primary functional entity is essential for the functioning of the MAMES Protocol and it refers to the forward link (from the MAMES Alert Provider to the MAMES Receiver), a secondary functional entity is optional and refers to the return link (from the MAMES Alert Receiver to the MAMES Alert Provider), therefore it is present only if MAMES runs over bidirectional networks.

Table 5.1: MAMES Main Functionalities

MAMES functional entity	General Description	MAMES Network Side	Agent-specific Description
MAMES Message Composition	MAMES Frame generation: creation of the MAMES Header and encapsulation of Alert Protocol Message(s) (if any) in the MAMES payload.	Alerter-Side	<ul style="list-style-type: none"> primary functional entity of the MAMES Alerter-Side Agent (MAMES Alert Provider); responsible for the generation of the MAMES Message to be transmitted over the (SatCom/SatNav/Com) network towards the MAMES Receiver (forward link).
		User-Side	<ul style="list-style-type: none"> secondary functional entity of MAMES User-Side Agent (MAMES Alert Receiver); responsible for the generation of the MAMES acknowledgements to be transmitted back to the MAMES Alert Provider (return link).
MAMES Message Parsing	MAMES Frame processing: parsing of the MAMES Header and decapsulation of the Alert Protocol Message(s) contained in the Payload (if any).	Alerter-Side	<ul style="list-style-type: none"> secondary functional entity of MAMES Alerter-Side Agent, complementary to the MAMES Message Composition functionality of the MAMES User-Side Agent; responsible for the processing of the received MAMES acknowledgement: parsing and proper handling of the decapsulated Alert Protocol Message(s), if any (return link).
		User-Side	<ul style="list-style-type: none"> primary functional entity MAMES User-Side Agent; responsible for the processing of the received MAMES Frame: check, parsing of the MAMES Message and proper handling of the decapsulated Alert Protocol Message(s), if any (forward link).
MAMES Scheduling & Forwarding	MAMES Frames Scheduling and forwarding towards the MAMES network entity the MAMES Message is destined to.	Alerter-Side	<ul style="list-style-type: none"> responsible for the scheduling of the generated MAMES Messages and forwarding to the appropriate queue for transmission (forward link).
		User-Side	<ul style="list-style-type: none"> responsible for the scheduling of the generated MAMES acknowledgement and forwarding to the appropriate queue for transmission (return link).

5.2 Protocol Architecture

5.2.1 MAMES Positioning in a Protocol-stack Architecture

The objective of this clause is to define the MAMES positioning in a protocol-stack architecture, assuming a generic satellite-based communications network (for terrestrial networks, the satellite-specific entities would have to be replaced by the corresponding terrestrial entities).

In terms of the OSI layer model, it is assumed that MAMES operates above the highest layer provided by the (satellite) dissemination network. Figure 5.1 illustrates a mapping to OSI Layers of the different entities involved in the Protocol Architecture. In detail:

- Only the alerter side of the Alert Network is shown in the figure, since the user side is analogous.
- The specification "local" indicates that the two entities are co-located, i.e. either integrated into a single device or directly attached.
- Since the focus of this Technical Specification is on alert-related layers, the "lower layers" are not considered in detail.
- The Alert Protocol Layer is typically located at the OSI Presentation Layer (L6) or the Application Layer (L7).
- The MAMES Layer is intended to accommodate various Alert Protocols and to work over different lower-layer technologies (from Data Link to Transport Layer). For this reason, it closely represents the OSI Session Layer (L5), but it borrows features from OSI Layers 4 to 7.

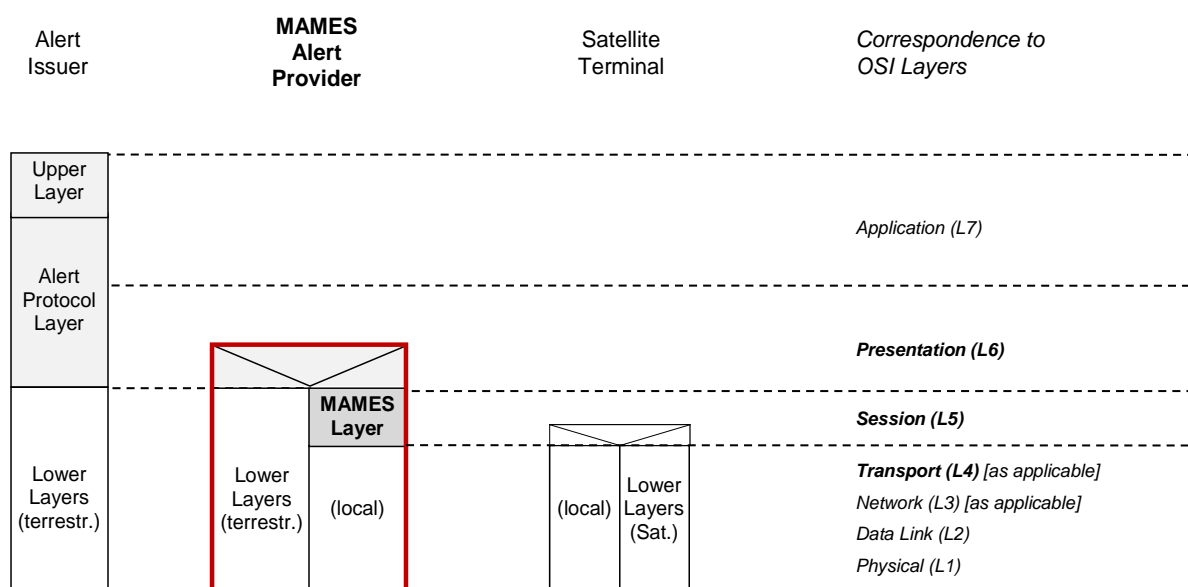


Figure 5.1: Mapping to OSI Layers

NOTE: Figure 5.1 is an approximate representation of the MAMES Layer mapping to the OSI Layers.

MAMES shall be implemented in the protocol stack as a protocol layer that:

- controls the dialogue between MAMES Entities (peers), establishing, managing and terminating communications between peers;
- offers the encapsulation service towards the above protocol layer, e.g. generating Alert Protocol Messages;
- acts as interface to the underlying layers that properly transport MAMES Message(s) through the network.

In the following a high level design of the MAMES protocol architecture is provided. In particular, focusing on the location of the termination points of the MAMES and of the Alert Protocol, four scenarios are identified and for each of them the protocol-stack architecture is reported. As highlighted in Table 5.2 the two considered criteria are:

- MAMES termination point is INSIDE/OUTSIDE the satellite user segment (Direct/Indirect MAMES Alerting) (*primary criterion*);
- MAMES and Alert Protocol termination points are co-located/not co-located (*secondary criterion*).

Table 5.2: MAMES Scenarios

	Direct MAMES Alerting	Indirect MAMES Alerting
Co-located MAMES and Alert Protocol terminations	Scenario A1	Scenario B1
Non co-located MAMES and Alert Protocol terminations	Scenario A2	Scenario B2

For the description of the Protocol Architecture, it is worth introducing the Alert Intermediary System (although it is not a MAMES entity), clarifying its role within the MAMES Network.

An Alert Intermediary System is defined as a telecommunication network or a node that forwards alert-related messages. An Alert Intermediary System can be represented by:

- a simple network relay node, which relays the received MAMES Message/Alert Protocol Message through a specific communication link and technology and re-transmits it over a different link and based on a different communication technology;
- a telecommunication network (based on any suitable technology), used for transporting MAMES Message/Alert Protocol Message.

Alert Intermediary Systems are only considered at the user side of the overall alert network, i.e. between the Satellite Terminal and the Alerting Device, as detailed in the Scenarios analysis reported in the following.

5.2.2 Protocol Architecture for Direct MAMES Alerting

5.2.2.1 Scenario A1

In Scenario A1 the MAMES Receiver is inside the satellite user segment and MAMES and Alert Protocol terminations are co-located (the Alerting Device and the MAMES Alert Receiver are co-located).

Figure 5.2 depicts the Scenario A1 protocol stack architecture.

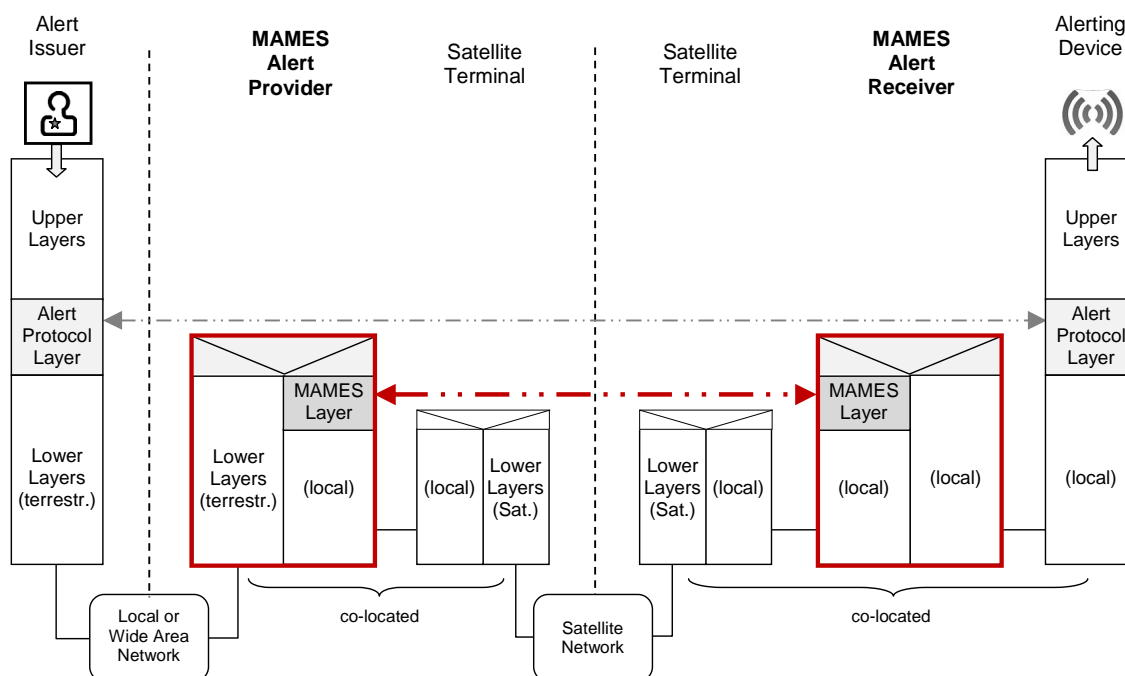


Figure 5.2: Protocol Architecture for Scenario A1

In detail: an Alert Protocol Message is sent by the Alert Issuer to the MAMES Alert Provider which is in charge of encapsulating the received Alert Protocol Message (through the MAMES Alerter-Side Agent) and distributing the generated MAMES Message using its associated satellite communication/navigation network. The MAMES Message is directly received by the satellite terminal co-located with the MAMES Receiver and the Alerting device, which are inside the satellite user segment. The MAMES Receiver decapsulates the Alert Protocol Message contained in the MAMES Message Payload (thanks to the embedded MAMES User-Side Agent) and sends it to the attached Alerting Device for Alert Protocol Message content interpretation and rendering.

Figure 5.3 shows the integrated version of the Scenario A1 Protocol Architecture. It presents the co-located entities as integrated entities, but from a protocol architecture point of view it is equivalent to Figure 5.2. The integrated version is reported as additional information only for scenario A1, although a corresponding integrated version could be represented for each of the identified scenarios.

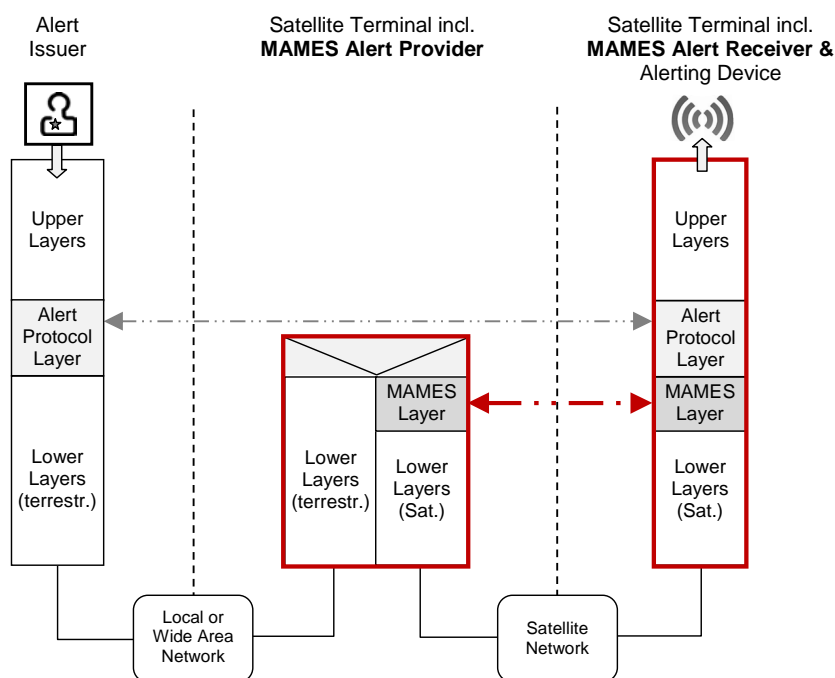


Figure 5.3: Protocol Architecture for Scenario A1 (integrated version)

5.2.2.2 Scenario A2

In Scenario A2 the MAMES Receiver is inside the satellite user segment, but the MAMES and Alert Protocol terminations are not co-located. The Alerting Device is outside the satellite user segment and it is connected to the MAMES Receiver via one or more Alert Intermediary Systems.

Figure 5.4 depicts the Scenario A2 protocol stack architecture.

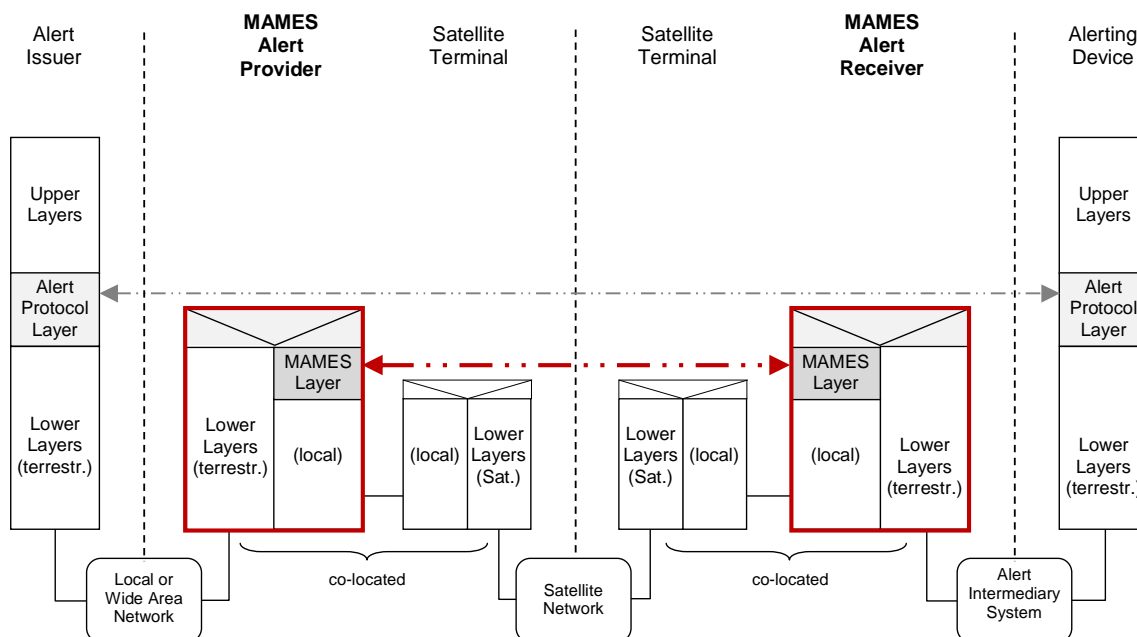


Figure 5.4: Protocol Architecture for Scenario A2

In detail: the MAMES Message is directly received by the satellite terminal co-located with the MAMES Alert Receiver. The MAMES Alert Receiver decapsulates the Alert Protocol Message contained in the MAMES Message Payload and sends it to the Alerting Device through the Alert Intermediary System, it is connected to. The Alert Intermediary System, which can be represented by a terrestrial network node, acts as a relay node that forwards the received Alert Protocol Messages to the Alerting Device, where they are interpreted and rendered.

As an example in the Figure 5.4 only one Alert Intermediary System is reported, however different Alert Intermediary Systems can be traversed by the Alert Protocol Messages before reaching the Alerting Device, which represents the termination point of the Alert Protocol.

5.2.3 Protocol Architecture for Indirect MAMES Alerting

5.2.3.1 Scenario B1

In Scenario B1 the MAMES Receiver is outside the satellite user segment and MAMES and Alert Protocol terminations are co-located.

Figure 5.5 depicts the Scenario B1 protocol stack architecture.

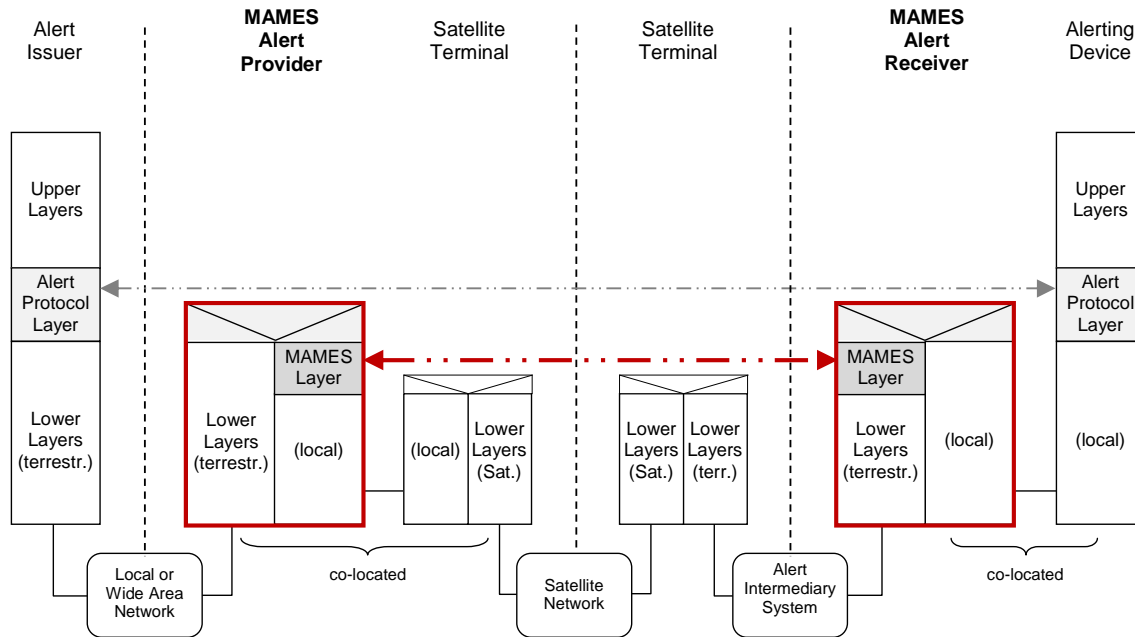


Figure 5.5: Protocol Architecture for Scenario B1

In detail: the MAMES Alert Provider generates the MAMES Message and transmits it using its associated satellite communication/navigation network. The MAMES Message is received by the satellite terminal and forwarded to an Alert Intermediary System that relays it to the MAMES Alert Receiver. The MAMES Receiver decapsulates the Alert Protocol Message contained in the MAMES Message Payload and sends it to the Alerting Device, it is attached to. The Alerting Device interprets and renders the Alert Protocol Messages.

NOTE: Differently from the Direct MAMES Alerting scenarios, in the figures depicting the Indirect MAMES Alerting scenarios the alert provider side ("Alert Issuer/MAMES Alert Provider") is not symmetric with the alert receiver side. However, this is not relevant for the carried out analysis.

5.2.3.2 Scenario B2

In Scenario B2 the MAMES Receiver is outside the satellite user segment and the MAMES and Alert Protocol terminations are not co-located. One or more Alert Intermediary Systems are in between the MAMES Alert Provider and the MAMES Alert Receiver (MAMES Message relaying) and between the MAMES Alert Receiver and the Alerting Device (Alert Protocol Messages relaying).

Figure 5.6 depicts the Scenario B2 protocol stack architecture.

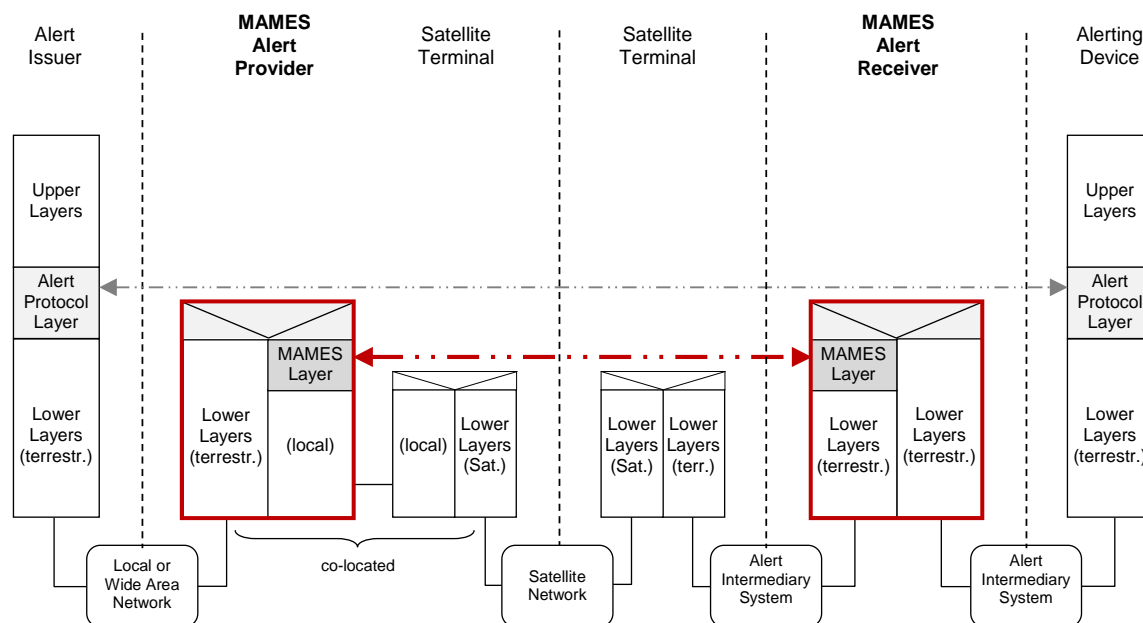


Figure 5.6: Protocol Architecture for Scenario B2

In detail: the MAMES Message is generated by the MAMES Alert Provider and transmitted over the attached satellite network. The MAMES Message is received by the satellite terminal and forwarded to an Alert Intermediary System that relays it to the MAMES Alert Receiver. The MAMES Receiver decapsulates the MAMES Message and forwards the Alert Protocol Messages to an Alert Intermediary System, which relays them to the Alerting Device for content interpretation and rendering.

As an example in the Figure 5.6 only two Alert Intermediary Systems are depicted, however different Alert Intermediary Systems can be traversed by the MAMES Message before reaching the MAMES Protocol termination point (MAMES Alert Provider - MAMES Alert Receiver segment) and by the Alert Protocol Messages, before reaching the Alert Protocol termination point (MAMES Alert Receiver - Alerting Device segment).

6 MAMES Messages

6.1 Overall Structure

The objective of this clause is to provide the definition of the MAMES Messages. Following a hierarchical organization, the MAMES message types are presented in clause 6.2, the headers are defined in clause 6.3 and details on the header fields are reported in clause 6.4.

To introduce the definition of the MAMES messages, Figure 6.1 illustrates the general structure of a MAMES Frame and the adopted notation.

A MAMES Frame is composed of:

- a set of MAMES Headers, which may comprise:
 - Mandatory Header (MH);
 - Extension Headers (EHs);
 - Alert Message Headers (AMHs);
- a MAMES Payload, comprising a concatenation of Alert Protocol Messages (zero, single or multiple Alert Protocol Messages).

An Alert Protocol Message can be a message formatted according to an advanced Alert Protocol (e.g. CAP, with several dedicated message types), or a simple message conforming to an arbitrary Internet Media Type.

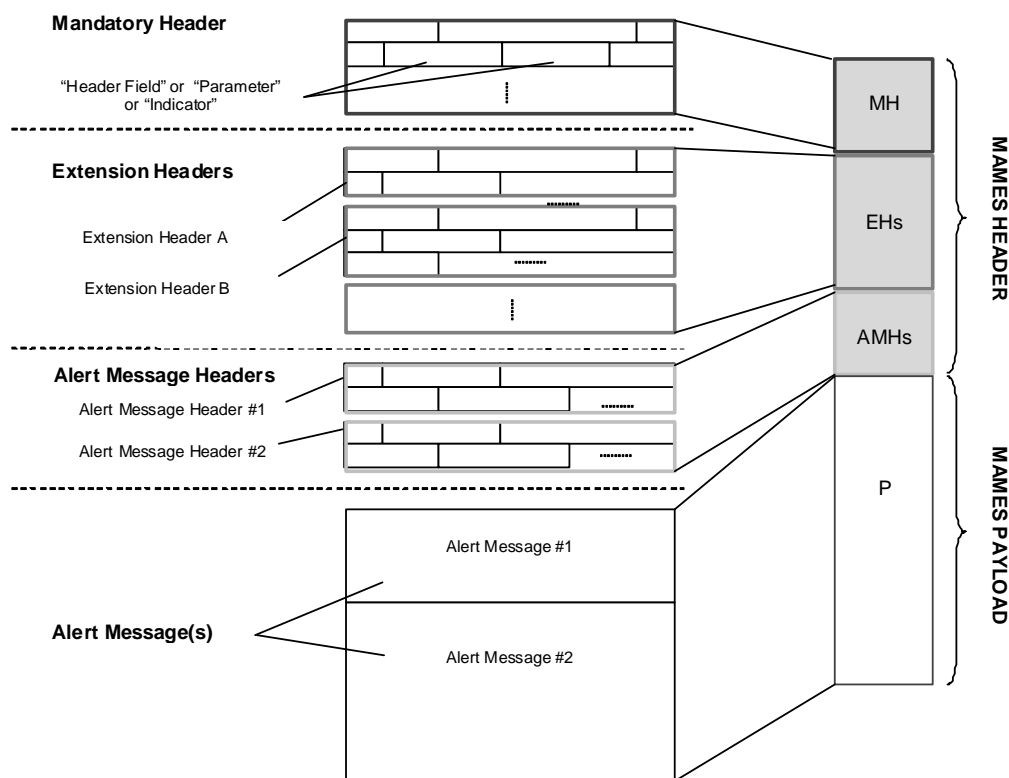


Figure 6.1: MAMES Frame Structure and Notation

To enable the encapsulation of multiple Alert Protocol Messages in a single MAMES Message, the following constraint shall be considered:

"One MAMES Message => one event => one event category => one Notification Area => one Alert Issuer => one issuance time".

This means that all the Alert Protocol Messages contained in a MAMES Payload shall:

- i) refer to a single event (incident) and belong to the same event category (e.g. meteorological, geophysical, etc.;
- ii) be destined to the same notification area;
- iii) be issued by one Alert Issuer in the same time instant.

However the encapsulation of a concatenation of multiple Alert Protocol Messages in the MAMES Payload allows to meet the different rendering capabilities of the Alerting Devices. In fact the encapsulated Alert Protocol Messages are characterized by different Alert Protocols or media types (text, audio, image, etc.) and by different languages or by no languages (e.g. for images).

NOTE: Some examples of MAMES Frames are given in annex C.

6.2 MAMES Message Types

6.2.1 Overview of MAMES Message Types

Different types of MAMES Message are defined based on the message purpose (e.g. message function) and satellite network transmission constraints (e.g. MAMES Transmission over GNSS Systems).

Five types of MAMES Messages are defined. These are:

- MAMES ALERT;
- MAMES Ultra-short ALERT (Us-ALERT);

- MAMES UPDATE;
- MAMES CANCEL;
- MAMES ACK.

In order to identify the type of MAMES Message an indicator is defined and it is named "MAMES Message Type".

Figure 6.2 provides an overview of the MAMES Message types, highlighting that the MAMES Ultra-short ALERT and the MAMES CANCEL types are characterized by an empty payload, while the other ones may or may not include a payload. Empty payload means that only the MAMES Header is transmitted. In detail for each MAMES Message Type the MAMES Header and the MAMES Payload are depicted and the Header field ("indicator") is shown within the MAMES Header of the different types of messages.

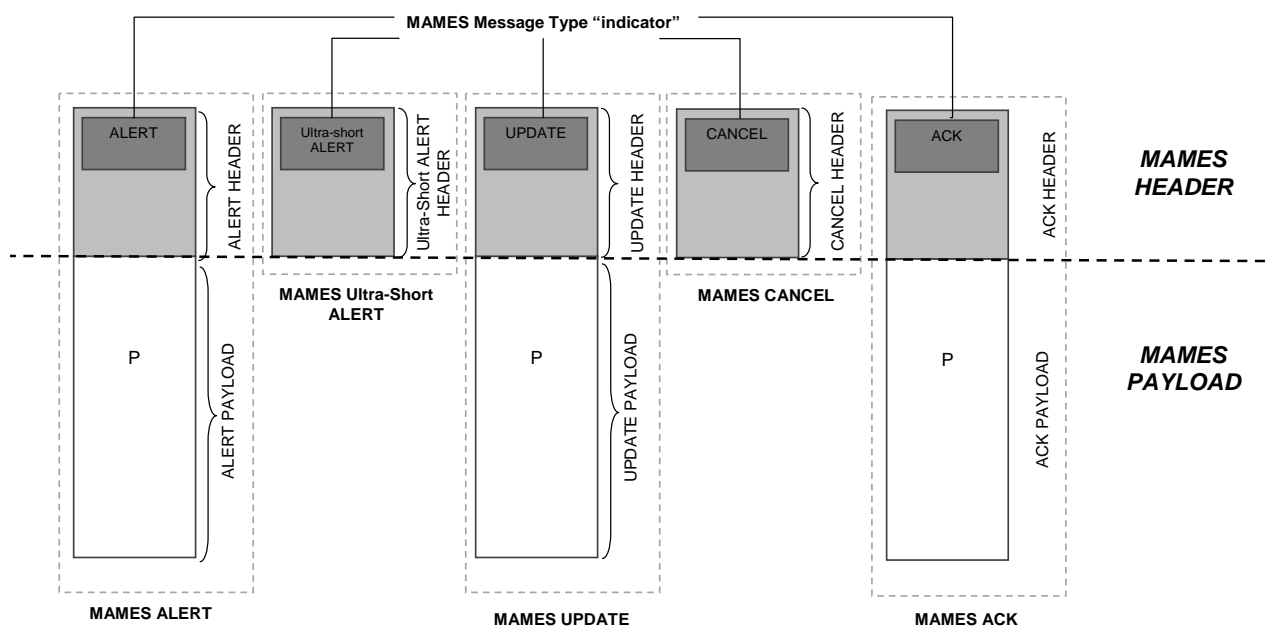


Figure 6.2: MAMES Message Classification

It is worth highlighting that upon the reception of an Alert Protocol Message issued by an Alert Issuer, a MAMES Alert Provider generates a MAMES Frame selecting one of the defined MAMES message types. This selection depends on one or more of the following factors (this will be better explained in clause 7):

- the instructions provided by the Alert Issuer;
- the availability of network resources the MAMES Alert Provider uses for the distribution of MAMES Messages.

Concerning the latter point, this information could be provided by the Alert Issuer, or it could be derived by the MAMES Alert Provider after trying to send the MAMES Frame to the underlying layer and having received an error message (e.g. return error, socket notification, etc.). In this case special actions will be taken by the MAMES Provider.

Moreover a MAMES Alert Provider may also generate MAMES Messages (MAMES UPDATE or MAMES CANCEL messages) on its own initiative for MAMES internal reasons, as the case of an erroneous transmission or the need of correcting a previously sent MAMES Message.

Further details are provided in the following clauses, where for each type of MAMES Message the scope and the basic functions are described.

6.2.2 MAMES ALERT

MAMES ALERT Message enables the encapsulation of a single or multiple Alert Protocol Messages that need to be delivered to the Alerting Device.

A MAMES ALERT:

- enables the encapsulation of different Alert Protocol Messages including all the Alert Protocol specific messages types (e.g. CAP cancel/update messages, which represents Alert Protocol level cancellation/updates of previously sent CAP messages);
- may include a payload: in "normal conditions", it includes at least one Alert Protocol Message in the payload.

Table 6.1 lists the MAMES ALERT components.

Table 6.1: MAMES ALERT Components

Components	Components Details	Optionality
ALERT Header	ALERT Mandatory Header (ALERT MH)	mandatory
	EHS	optional
	AMHs	conditional (present if an Alert Message is present: there will be one AMH per AM)
Payload	single or multiple Alert Protocol Messages	optional

6.2.3 MAMES Ultra-Short ALERT

The MAMES Ultra-short Message is the shortest MAMES Message defined with the aim to allow the transmission of MAMES Messages over narrowband satellite channels (e.g.: MAMES over GNSS).

A MAMES Ultra-short ALERT:

- is an extreme solution used in exceptional cases (e.g.: network resources limited contexts, out-of-band signaling, etc.);
- carries very limited information;
- does not include backward/forward reference to a "longer" MAMES Message (MAMES ALERT).

A MAMES Ultra-short ALERT Message consists of only a Header, the Ultra-short ALERT Mandatory Header (Us-ALERT MH).

6.2.4 MAMES UPDATE

MAMES UPDATE Message is an update at MAMES level. It is an update of a valid previously transmitted MAMES Message (MAMES ALERT or MAMES UPDATE).

A MAMES UPDATE:

- handles updates at MAMES level enabling the encapsulation of those Alert Protocol Messages that do not include at Alert Protocol level a means to identify a message as an update or a cancellation of a previously sent Alert Protocol Message;
- overwrites the Headers/Payload of the MAMES Frame it refers to, and leaves Headers/Payload that are not included unchanged;
- may include a payload.

NOTE: Details on the actions performed by the MAMES Alert Provider to update alert information are reported in clause 7 and in [i.1].

Table 6.2 lists the MAMES UPDATE components.

Table 6.2: MAMES UPDATE Components

Components	Components Details	Optionality
UPDATE Header	UPDATE Mandatory Header (UPDATE MH)	mandatory
	EHs (the ones that need to be updated)	optional
	AMHs (the ones pertaining to the AMs that need to be updated)	conditional (present if an Alert Message is present: there will be one AMH per AM)
Payload	single or multiple Alert Protocol Messages (updated versions of the Alert Protocol Messages contained in the MAMES Message the MAMES UPDATE refers to)	optional

6.2.5 MAMES CANCEL

A MAMES CANCEL Message is a cancellation at MAMES level. It declares a valid previously transmitted MAMES Message (MAMES ALERT, MAMES Ultra-short ALERT, MAMES UPDATE) as obsolete.

MAMES CANCEL handles MAMES errors enabling a MAMES Alert Provider to notify the MAMES Alert Receiver that a previous sent MAMES Message shall be considered obsolete and shall not be forwarded to the Alerting Device anymore (as in case of an erroneous transmission of a MAMES Message due to e.g. human/machine error, unauthorized transmission, incorrect formatting).

A MAMES CANCEL consists of only a header (CANCEL Header); Table 6.3 lists the CANCEL Header components.

NOTE 1: In case of a temporary unavailability of network resources (which makes the MAMES Alert Provider use only MAMES Ultra-short ALERT Frames), if a previously sent MAMES Message (MAMES ALERT or UPDATE) needs to be updated, the MAMES Alert Provider: i) declares the previously sent MAMES Message as obsolete by sending a MAMES CANCEL; ii) sends a MAMES Ultra-short ALERT Frame.

NOTE 2: MAMES CANCEL can be used to cancel a MAMES Ultra-short ALERT.

NOTE 3: Details on the actions performed by the MAMES Alert Provider to handle MAMES errors are reported in clause 7 and in [i.1].

Table 6.3: MAMES CANCEL Header Components

Components	Components Details	Optionality
CANCEL Header	CANCEL Mandatory Header (CANCEL MH)	mandatory
	EHs	optional

6.2.6 MAMES ACK

The MAMES ACK message provides acknowledgement at MAMES level of a previously received MAMES Message (ALERT or UPDATE, or CANCEL messages).

MAMES ACK:

- notifies the success of reception of a MAMES Message;
- is transmitted from the MAMES Receiver to the MAMES Provider in case a return link is available (bidirectional SatCom/Com network) and the MAMES Alert Provider asks for acknowledgement or an Alert Protocol level acknowledgement needs to be transmitted;
- enables the encapsulation of Alert Protocol level acknowledgements (only in this case the MAMES ACK includes a payload).

Table 6.4 lists the MAMES ACK components.

Table 6.4: MAMES ACK Components

Components	Components Details	Optionality
ACK Header	ACK Mandatory Header (ACK MH)	mandatory
	EHs	optional
	AMHs (the ones pertaining to the AMs that need to be acknowledged)	conditional (present if an Alert Message is present: there will be one AMH per AM)
Payload	Alert Protocol acknowledgement messages type of the Alert Protocol Messages contained in the MAMES Message the MAMES ACK refers to	conditional (present if an Alert Protocol acknowledgement message type needs to be transmitted back to the Alert Issuer)

6.3 MAMES Message Headers

6.3.1 MAMES Mandatory Headers

6.3.1.1 General Features

The main general features that characterize the MAMES Mandatory Headers of all the defined MAMES Message types follow. A Mandatory Header:

- is mandatory;
- is of fixed length;
- pertains to the entire MAMES Message;
- shall be processed by every MAMES Agent.

6.3.1.2 The ALERT Mandatory Header

Table 6.5: ALERT Mandatory Header

MAMES Header Type	ALERT Mandatory Header
Definition	Mandatory Header of the MAMES ALERT Frame.
Header Fields	MAMES Protocol Version
	MAMES Message Type
	MAMES Message ID
	MAMES Alert Provider ID
	Notification Area
	MAMES Transport Priority
	ACK Request Indicator
	Alert Issuer ID
	Next Header Type

6.3.1.3 The Ultra-Short ALERT Mandatory Header

Table 6.6: Ultra-short ALERT Mandatory Header

MAMES Header Type	Ultra-short ALERT Mandatory Header
Definition	Mandatory Header of the MAMES Ultra-short ALERT Frame. It represents the entire MAMES Ultra-short ALERT Frame.
Header Fields	MAMES Protocol Version
	MAMES Message Type
	MAMES Message ID
	MAMES Alert Provider ID
	Notification Area
	MAMES Transport Priority
	Alert Issuer ID
	MAMES Event Category

6.3.1.4 The UPDATE Mandatory Header

Table 6.7: UPDATE Mandatory Header

MAMES Header Type	UPDATE Mandatory Header
Definition	Mandatory Header of the MAMES UPDATE Frame.
Header Fields	MAMES Protocol Version
	MAMES Message Type
	MAMES Message ID
	MAMES Alert Provider ID
	Notification Area
	MAMES Transport Priority
	MAMES Reference
	ACK Request Indicator
	Alert Issuer ID
	Next Header Type

6.3.1.5 The CANCEL Mandatory Header

Table 6.8: CANCEL Mandatory Header

MAMES Header Type	CANCEL Mandatory Header
Definition	Mandatory Header of the MAMES CANCEL Frame.
Header Fields	MAMES Protocol Version
	MAMES Message Type
	MAMES Message ID
	MAMES Alert Provider ID
	Notification Area
	MAMES Transport Priority
	MAMES Reference
	ACK Request Indicator
	Next Header Type

6.3.1.6 The ACK Mandatory Header

Table 6.9: ACK Mandatory Header

MAMES Header Type	ACK Mandatory Header
Definition	Mandatory Header of the MAMES ACK Frame.
Header Fields	MAMES Protocol Version
	MAMES Message Type
	MAMES Reference
	MAMES Alert Provider ID
	MAMES User Location
	MAMES Transport Priority
	Alert Issuer ID
	MAMES Receiver ID
	Next Header Type

6.3.2 MAMES Extension Headers

6.3.2.1 General Features

The main general features that characterize all the defined MAMES Extension Headers follow. An EH:

- aims at enhancing the MAMES Frame by adding new features (e.g. integrity, encryption, etc.);
- is an optional header of the MAMES Message;
- pertains to the entire MAMES Message;

- may contain fixed or variable length fields; for each variable length field, a field indicating its length is present;
- contains only mandatory fields;
- shall contain a "Next Header Type" field, specifying the type of the next header.

A concatenation of multiple EHs is permitted. There is no mandated ordering of the headers.

For each EH a rotated version of the same header is defined (see annex D), the rotated version contains the same fields as the non-rotated one, but placed and ordered in a different way. In order to guarantee a 32-bits alignment of the fields, the concatenation of the EHs shall be performed according to the algorithm specified in clause 6.3.4.

6.3.2.2 Alert and Response Type Header

Table 6.10: Alert and Response Type Header

MAMES Extension Header	Alert and Response Type Header
Definition	It denotes the appropriate handling and the intended distribution of the MAMES message and provides information on the category of the incident and the recommended type of action.
Header Fields	MAMES Status MAMES Alert Scope MAMES Response Type MAMES Event Category Next Header Type
Allowed in MAMES Message Types	ALERT; UPDATE; CANCEL

6.3.2.3 Incident Header

Table 6.11: Incident Header

MAMES Extension Header	Incident Header
Definition	It denotes the incident ID and the time when the alert was (first) issued by the Alert Issuer.
Header Fields	MAMES Incident ID Issuance Time Next Header Type
Allowed in MAMES Message Types	ALERT; UPDATE; CANCEL

6.3.2.4 Validity Header

Table 6.12: Validity Header

MAMES Extension Header	Validity Header
Definition	It denotes the start and end time validity of the MAMES Message.
Header Fields	MAMES Validity Start MAMES Validity End Next Header Type
Allowed in MAMES Message Types	ALERT; UPDATE; CANCEL

6.3.2.5 Administrative Areas Header

Table 6.13: Administrative Areas Header

MAMES Extension Header	Administrative Areas Header
Definition	It denotes the Administrative Area(s) to be alerted.
Header Fields	Administrative Areas Header Version
	Administrative Areas Coding
	Number of Areas
	Area IDs
	Next Header Type
Allowed in MAMES Message Types	ALERT; UPDATE; CANCEL

6.3.2.6 Authentication/Integrity Header

When performing authentication or integrity procedures, the provisions described in the ISO/IEC 27000 family of standards should be followed (see e.g. ISO/IEC 27000:2014 [i.2]). A comprehensive list of recommended algorithms is provided by NIST [i.3].

All MAMES Headers, except the Authentication/Integrity Header itself, and the MAMES Payload should be authenticated by means of the specified algorithm. Any encryption procedures at the MAMES Alert Provider shall be carried out after authentication.

Table 6.14: Authentication/Integrity Header

MAMES Extension Header	Authentication/Integrity Header
Definition	It is used for Authentication/Integrity.
Header Fields	Authentication/Integrity Header Version
	Authentication/Integrity Flag
	Authentication/Integrity Algorithm ID
	MAC Value Length
	MAC Value
	Next Header Type
Allowed in MAMES Message Types	ALERT; UPDATE; CANCEL; ACK

6.3.2.7 Encryption Header

When performing encryption procedures, the provisions described in the ISO/IEC 27000 family of standards should be followed (see e.g. ISO/IEC 27000:2014 [i.2]). A comprehensive list of recommended algorithms is provided by NIST [i.3].

Only the MAMES Payload should be encrypted by means of the specified algorithm. Any authentication or integrity procedures should be carried out before encryption.

Table 6.15: Encryption Header

MAMES Extension Header	Encryption Header
Definition	It is used for Encryption.
Header Fields	Encryption Header Version
	Encryption Algorithm ID
	Initialization Vector Length
	Initialization Vector
	Block Size
	Number of Padding Bytes
	Next Header Type
	Allowed in MAMES Message Types

6.3.3 The Alert Message Header

Table 6.16: Alert Message Header

MAMES Header Type	Alert Message Header
Definition	Alert Protocol Message specific header. It denotes the presence of at least one Alert Protocol Message in the MAMES Payload and it provides information related to that Alert Protocol Message.
Header Fields	Alert Message Type
	Language ID
	Alert Message Length
	More AMHs Flag
Allowed in MAMES Message Types	ALERT; UPDATE; ACK

As for the EHs, a rotated version of the AMH is defined (see annex D) to guarantee a 32-bit alignment of the fields in the concatenation of different EHs and AMHs. The concatenation headers algorithm is specified in clause 6.3.4.

6.3.4 MAMES Headers Concatenation Algorithm

The objective of this clause is to define the algorithm to be followed for concatenating the different defined MAMES Headers types, guaranteeing 32-bits alignment of their fields.

Two assumptions are the basis of the defined algorithm. These are:

- every MAMES header type (MH, EHs, AMH) is aware of its size;
- all the MAMES header types shall be aligned to 16-bits if they are not reserved bits are added (see annex D for details).

Under these assumptions it may occur that:

- a MAMES Header type is composed of an odd number of half words (a word is 32 bits long);
- a MAMES Header type is composed of an even number of half words;

For the only purpose of the definition of the concatenation algorithm, the MAMES Header types that belong to the former category are called H1 headers, while the ones that belong to the latter category are named H2 headers.

The algorithm relies on the definition of two header versions for the H1 headers: a *non-rotated* and a *rotated* version (as defined in annex D).

Table 6.17 lists all the possible concatenation cases and the way of concatenating the headers. In detail, the identified cases depend on the MAMES header types that need to be concatenated (X and Y in table); the action to be performed (if any) and the version to be used are reported in the last column.

Table 6.17: MAMES Headers Concatenation Algorithm

Case	Previous MAMES Header Type (X)	MAMES Header Type to be concatenated (Y)	Algorithm
1	H1	H1	The <i>rotated</i> version of Y shall be used.
2	H1	H2	16 reserved bits are added and the <i>non-rotated</i> version of Y shall be used.
3	H2	H1	The <i>non-rotated</i> version of Y shall be used.
4	H2	H2	The <i>non-rotated</i> version of Y shall be used.

6.4 MAMES Header Fields

6.4.1 Fields of Mandatory Headers

6.4.1.1 MAMES Protocol Version

Table 6.18: MAMES Protocol Version Field

Field Name	MAMES Protocol Version		
Definition	Version of the MAMES protocol used for Alert Protocol Message(s) encapsulation.		
Code values	Field Length [bits]	Value Range [decimal]	Description
	4	0 ≤ version ≤ 15	Version number of the MAMES Protocol.

6.4.1.2 MAMES Message Type

Table 6.19: MAMES Message Type Field

Field Name	MAMES Message Type		
Definition	Type of the MAMES Message.		
Code values	Five codes are used to identify the different MAMES Message types.		
	Field Length [bits]	Value Range [binary]	Description
4	4	0100	MAMES ALERT
		0001	MAMES UPDATE
		0010	MAMES CANCEL
		0011	MAMES ACK
		0000	Ultra-short MAMES ALERT
		(all other)	(reserved)

6.4.1.3 MAMES Message ID

Table 6.20: MAMES Message ID Field

Field Name	MAMES Message ID		
Definition	Unique identifier of a MAMES Frame originated by a MAMES Alert Provider.		
Code values	The MAMES Alert Provider is responsible for the numbering of MAMES Messages. Consecutive numbers are used.		
	Field Length [bits]	Value Range [binary]	Description
12	12	000000000000	First MAMES Message sent by the MAMES Alert Provider A
		000000000001	Second MAMES Message sent by the MAMES Alert Provider A.
	
		111111111111	Last MAMES Message sent by the MAMES Alert Provider A, before restarting from 000000000000 MAMES Message ID.

6.4.1.4 MAMES Alert Provider ID

Table 6.21: MAMES Alert Provider ID Field

Field Name	MAMES Alert Provider ID		
Definition	Identifier of the sender of the MAMES Message (MAMES Alert Provider).		
Code values	Each MAMES Alert Provider is identified by a binary coded number:		
	Field Length [bits]	Value Range [binary]	Description
	12	000000000000	MAMES Alert Provider A
		000000000001	MAMES Alert Provider B
	

6.4.1.5 Notification Area

Table 6.22: Notification Area Field

Field Name	Notification Area			
Definition	Geographic area where the MAMES Message needs to be delivered. It is represented by a circle and it is specified by: a circle center (latitude and longitude) and a radius (index).			
Code values	The code value identifying the Notification Area is implemented as a bit array consisting of the sub-code fields listed in the following. An example is provided in clause B.1.1.			
	Field Length [bits]	Sub-code bit size	Value Range [decimal]	
	48	1	0-1	Latitude North/South (+/-) (1/0)
		7	0-89	Latitude Degrees
		6	0-59	Latitude Minutes
		6	0-59	Latitude Seconds
		1	0-1	Longitude East/West (+/-) (1/0)
		8	0-179	Longitude Degrees
		6	0-59	Longitude Minutes
		6	0-59	Longitude Seconds
4		0-15	Radius Index (up to 2 000 km & >2 000 km).	
3		(all other)	(reserved)	

NOTE: The radius indexes are detailed in clause B.1.1.

6.4.1.6 MAMES Transport Priority

Table 6.23: MAMES Transport Priority Field

Field Name	MAMES Transport Priority		
Definition	Priority of the MAMES Frame with respect to other MAMES Frames at transport level. It shall not be understood as priority of the Alert Protocol Message.		
Code values	Two MAMES Priority levels are defined.		
	Field Length [bits]	Value Range [binary]	Description
	2	01	Expedited - The MAMES Message should be sent immediately.
		00	Best effort - The MAMES Message should be sent according to a best effort mechanism. This represents also the case of MAMES Message with an unspecified priority.
(all other)		(reserved)	

6.4.1.7 ACK Request Indicator

The ACK should be intended as a delivery report, i.e. as a way to get rough information on the distribution of the alerts. If the ACK is not requested, then no MAMES message shall be sent on the return link, this means that also Alert-Protocol acknowledgments will not be forwarded by the MAMES Alert Receiver.

Table 6.24: ACK Request Indicator Field

Field Name	ACK Request Indicator		
Definition	Indicator of a MAMES ACK request from the MAMES Alert Provider.		
Code values	Field Length [bits]	Value Range [binary]	Description
	1	0	The MAMES Alert Receiver shall NOT send a MAMES ACK.
		1	The MAMES Alert Receiver may send a MAMES ACK.

6.4.1.8 Alert Issuer ID

Table 6.25: Alert Issuer ID Field

Field Name	Alert Issuer ID		
Definition	Identifier of the (original) source of the Alert Protocol Message, i.e. the emergency authority.		
Code values	Each MAMES Alert Issuer is identified by a binary coded number:		
	Field Length [bits]	Value Range [binary]	Description
	16	0000000000000000	MAMES Alert Issuer Unspecified
		0000000000000001	MAMES Alert Issuer A
		0000000000000010	MAMES Alert Issuer B
...		...	

6.4.1.9 Next Header Type

Table 6.26: Next Header Type Field

Field Name	Next Header Type		
Definition	Identifier of the type of the next header (header that immediately follows the current header).		
Code values	Field Length [bits]	Value Range [binary]	Description
	4	0001	Alert and Response Type Header
		0010	Incident Header
		0011	Validity Header
		0100	Administrative Areas Header
		0101	Authentication/Integrity Header
		0111	Encryption Header
		1000	Alert Message Header
		0000	No more headers follow.
		(all other)	(reserved)

6.4.1.10 MAMES Reference

Table 6.27: MAMES Reference Field

Field Name	MAMES Reference		
Definition	"MAMES Message ID" of an earlier MAMES Message, which needs to be referenced.		
Code values	See also "MAMES Message ID" code values definition - Clause 6.3.1.3)		
	Field Length [bits]	Value Range [binary]	Description
	12	000000000001	Reference to the first MAMES Message sent by the MAMES Alert Provider A
		000000000010	Reference to the second MAMES Message sent by the MAMES Alert Provider A.
...	

6.4.1.11 MAMES Receiver Location

Table 6.28: MAMES Receiver Location Field

Field Name	MAMES Receiver Location			
Definition	Geographical position of the sender (MAMES Receiver) of the MAMES ACK.			
Code values	The code value identifying the MAMES Receiver Location is implemented as a bit array consisting of the sub-code fields listed in the following. The code values cover the entire surface of the earth with an accuracy of 1 sec. (lat./long.), i.e. a few tens of meters. A code value for "unspecified" location is defined.			
	Field Length [bits]	Sub-code bit size	Value Range [decimal]	
48		1	0-1	Latitude North/South (+/-) (1/0)
		7	0-89	Latitude Degrees
		6	0-59	Latitude Minutes
		6	0-59	Latitude Seconds
		1	0-1	Longitude East/West (+/-) (1/0)
		8	0-179	Longitude Degrees
		6	0-59	Longitude Minutes
		6	0-59	Longitude Seconds
		7	(all other)	(reserved)
	0xffff ffff ffff (hexadecimal)		Code used for "unspecified" location	

6.4.1.12 MAMES Receiver ID

Table 6.29: MAMES Receiver ID Field

Field Name	MAMES Receiver ID		
Definition	Identifier of the sender of the MAMES ACK.		
Code values	The defined "MAMES Receiver ID" code values have local significance (each MAMES Alert Provider has its own ones).		
	Field Length [bits]	Value Range [binary]	Description
16		0000000000000000	Unspecified
		0000000000000001	MAMES User 1
		0000000000000010	MAMES User 2
		...	

6.4.2 Fields of Alert and Response Type Header

6.4.2.1 MAMES Status

Table 6.30: MAMES Status Field

Field Name	MAMES Status		
Definition	Status of the MAMES Message, denoting the appropriate handling of the MAMES Message (Actual - Exercise - System - Test).		
Code values	Four MAMES Status cases are defined.		
	Field Length [bits]	Value Range [binary]	Description
3		000	Actual (default): The MAMES Frame refers to an actual event.
		001	Exercise: The MAMES Frame refers to an exercise, rather than an actual emergency.
		010	System: The MAMES Frame is sent for system-internal purposes, rather than referring to an actual emergency.
		011	Test: The MAMES Frame is sent for test purposes.
		(all other)	(reserved)

6.4.2.2 MAMES Alert Scope

Table 6.31: MAMES Alert Scope Field

Field Name	MAMES Alert Scope		
Definition	Intended distribution of the MAMES message (restricted, unrestricted).		
Code values	Two MAMES Alert Scope code values are defined.		
	Field Length [bits]	Value Range [binary]	Description
	3	000	Public (default): The MAMES Frame is addressed to the general public, for unrestricted access.
		001	Restricted: The MAMES Frame is addressed to restricted audiences (e.g. emergency personnel or other authorities), rather than the general public.
(all other)		(reserved)	

6.4.2.3 MAMES Response Type

Table 6.32: MAMES Response Type Field

Field Name	MAMES Response Type		
Definition	Type of action recommended for the target audience: Shelter - Evacuate - Prepare - Execute - Avoid - Monitor - Assess - AllClear - None)		
Code values	Nine MAMES Response Type code values are defined.		
	Field Length [bits]	Value Range [binary]	Description
	4	0001	Shelter: Take shelter (details may be in the MAMES Payload).
		0010	Evacuate: Evacuate the area (details may be in the MAMES Payload).
		0011	Prepare: Make preparations (details may be in the MAMES Payload).
		0100	Execute: Execute a pre-planned activity (details may be in the MAMES Payload).
		0101	Avoid: Avoid the subject event (details may be in the MAMES Payload).
		0110	Monitor: Attend to information sources (details may be in the MAMES Payload).
		0111	Assess: Evaluate the information contained in the MAMES Payload.
		0111	AllClear: The subject event no longer poses a threat or concern and any follow-on action may be described in the MAMES Payload.
0000		None: No action recommended.	
(all other)	(reserved)		

6.4.2.4 MAMES Event Category

Table 6.33: MAMES Event Category Field

Field Name	MAMES Event Category		
Definition	Identifier of the event (incident) category.		
Code values	Thirteen MAMES Event Category code values are defined.		
	Field Length [bits]	Value Range [binary]	Description
4		0001	Geophysical (inc. landslide)
		0010	Meteorological (inc. flood)
		0011	General emergency and public safety
		0100	Law enforcement, military, homeland and local/private security
		0101	Rescue and recovery
		0110	Fire suppression and rescue
		0111	Medical and public health
		1000	Pollution and other environmental
		1001	Public and private transportation
		1010	Utility, telecommunication, other non-transport infrastructure
		1011	Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack (CBRNE)
		1100	Other events
		0000	The event is NOT specified.
	(all other)	(reserved)	

6.4.3 Fields of Incident Header

6.4.3.1 MAMES Incident ID

Table 6.34: MAMES Incident ID Field

Field Name	MAMES Incident ID		
Definition	Identifier of the incident. It is assigned by the MAMES Alert Provider for the purposes of identification and/or later reference.		
Code values	The defined "MAMES Incident ID" code values have local significance (each MAMES Alert Provider has its own ones).		
	Field Length [bits]	Value Range [decimal]	Description
8		0	Unspecified
		$1 \leq ID \leq 255$	Value assigned by the MAMES Alert Provider to identify the particular incident.

6.4.3.2 Issuance Time

Table 6.35: Issuance Time Field

Field Name	Issuance Time			
Definition	Time instant when the respective Alert was issued by the Alert Issuer.			
Code values	The code value is implemented as a bit array consisting of the sub-code fields listed in the following. The sub codes are strung together one after the other without separator. All date/time values between 1 Jan. 2000 0h 0' 0" and 31 Dec. 2255 23h 59' 59" . UTC A code value for "unspecified" issuance time is defined.			
	Field Length [bits]	Sub-code bit size	Value Range [decimal]	
	32	9	0-255	year since 2000
		4	1-12	month of the year
		5	1-31	day of the month
		5	0-23	hour of the day
		6	0-59	minute
3		0-7	Fraction of minute (10 seconds). In detail the following values are defined: "0" : from 0 to 9 seconds "1": from 10 to 19 seconds "2": from 20 to 29 seconds "3": from 30 to 39 seconds "4": from 40 to 49 seconds "5": from 50 to 59 seconds	
	0	Unspecified		

6.4.4 Fields of the Validity Header

6.4.4.1 MAMES Validity Start

Table 6.36: MAMES Validity Start Field

Field Name	MAMES Validity Start		
Definition	Time instant when the MAMES Frame shall become valid.		
Code values	For details see Table 6.35.		
	Field Length [bits]	Value Range	Description
	32	All date/time values between 1 Jan. 2000 0h 0' 0" and 31 Dec. 2255 23h 59' 59"	Code value (bit array) indicating the time instant when the MAMES Frame shall become valid.
	0	Unspecified	

6.4.4.2 MAMES Validity End

Table 6.37: MAMES Validity End Field

Field Name	MAMES Validity End		
Definition	Time instant when the MAMES Frame shall become invalid.		
Code values	For details see Table 6.35.		
	Field Length [bits]	Value Range	Description
	32	All date/time values between 1 Jan. 2000 0h 0' 0" and 31 Dec. 2255 23h 59' 59"	Code value (bit array) indicating the time instant when the MAMES Frame shall become invalid.
	0	Unspecified	

6.4.5 Fields of the Administrative Areas Header

6.4.5.1 Administrative Areas Header Version

Table 6.38: Administrative Areas Header Version Field

Field Name	Administrative Areas Header Version		
Definition	Version of the Administrative Areas Header.		
Code values	Field Length [bits]	Value Range [decimal]	Description
	4	$0 \leq \text{version} \leq 15$	Version number of the Administrative Areas Header

6.3.5.2 Administrative Areas Coding

Table 6.39: Administrative Areas Coding Field

Field Name	Administrative Areas Coding		
Definition	Identifier of the administrative areas coding scheme.		
Code values	Three Administrative Areas Coding schemes are supported by MAMES and corresponding code values are defined.		
	Field Length [bits]	Value Range [binary]	Description
	4	0000	NUTS [i.4]
		0001	LAU [i.5]
		0010	ISO 3166-1 [i.6]
(all other)		(reserved)	

6.4.5.3 Number of Areas

Table 6.40: Number of Areas Field

Field Name	Number of Areas		
Definition	Number of administrative area IDs contained in the <i>Area IDs</i> field.		
Code values	Field Length [bits]	Value Range [decimal]	Description
	6	$1 \leq \text{number} \leq 63$	The allowed maximum number of Area IDs is set to 63.
		0	Forbidden

6.4.5.4 Area IDs

Table 6.41: Area IDs Field

Field Name	Area IDs		
Definition	Identifiers of the administrative area codes of the scheme specified in the <i>Administrative Areas Coding</i> field.		
Code values	For each administrative areas coding scheme (defined by the Administrative Areas Coding field), a table mapping each administrative area code on a numeric index is provided in clause B.2. The numeric index is identified as the <i>Area ID</i> parameter. The code value is implemented as a bit array consisting of as many numeric indexes of administrative areas as denoted by the <i>Number of Areas</i> field, strung together one after the other without separator.		
	Field Length [bits]	Value Range	Description
	The field length is determined by the length of one area code, as derived from the <i>Administrative Areas Coding</i> field, multiplied by the <i>Number of Areas</i> parameter.	Any value of the specified length	Numeric indexes of the administrative area codes, strung together without separator.

6.4.6 Fields of the Authentication/Integrity Header

6.4.6.1 Authentication/Integrity Header Version

Table 6.42: Authentication/Integrity Header Version Field

Field Name	Authentication/Integrity Header Version		
Definition	Version of the Authentication/Integrity Header.		
Code values	Field Length [bits]	Value Range [decimal]	Description
	4	$0 \leq \text{version} \leq 15$	Version number of the Authentication/Integrity Header.

6.4.6.2 Authentication/Integrity Flag

Table 6.43: Authentication/Integrity Flag Field

Field Name	Authentication/Integrity Flag		
Definition	Flag denoting if an Authentication or an Integrity mechanism is applied to the MAMES Message.		
Code values	Field Length [bits]	Value Range [binary]	Description
	1	0	A MAMES Authentication mechanism is being applied.
		1	A MAMES Integrity mechanism is being applied.

6.4.6.3 Authentication/Integrity Algorithm ID

Table 6.44: Authentication/Integrity Algorithm ID Field

Field Name	Authentication/Integrity Algorithm ID		
Definition	Identifier of the employed authentication/integrity algorithm.		
Code values	Three Authentication/Integrity Algorithms are supported by MAMES and corresponding code values are defined.		
	Field Length [bits]	Value Range [binary]	Description
	6	000000	HMAC-SHA1 (as specified in [1])
		000001	HMAC-SHA256 (as specified in [2])
		000010	AES-CMAC (as specified in [3] and [4])
(all other)		(reserved)	

6.4.6.4 MAC Value Length

Table 6.45: MAC Value Length Field

Field Name	MAC Value Length		
Definition	Length of the Message Authentication Code value (in Bytes).		
Code values	Field Length [bits]	Value Range [decimal]	Description
	5	$1 \leq \text{length} \leq 31$	The length of the MAC Value is specified in terms of an integer, non-zero number of Bytes.
		0	Forbidden

6.4.6.5 MAC Value

Table 6.46: MAC Value Field

Field Name	MAC Value		
Definition	Value of the Message Authentication Code.		
Code values	Field Length [bits]	Value Range	Description
	As specified by the "MAC Value Length" parameter	Any value of the specified length	The output value resulting from the computations according to the Authentication/Integrity algorithm employed.

6.4.7 Fields of the Encryption Header

6.4.7.1 Encryption Header Version

Table 6.47: Encryption Header Version Field

Field Name	Encryption Header Version		
Definition	Version of the Encryption Header.		
Code values	Field Length [bits]	Value Range [decimal]	Description
	4	$0 \leq \text{version} \leq 15$	Version number of the Encryption Header.

6.4.7.2 Encryption Algorithm ID

Table 6.48: Encryption Algorithm ID Field

Field Name	Encryption Algorithm ID		
Definition	Identifier of the employed encryption algorithm.		
Code values	Two Encryption algorithms are supported by MAMES and corresponding code values are defined.		
	Field Length [bits]	Value Range [binary]	Description
	6	000000	AES-CBC (as specified in [5])
		000001	AES-CTR (as specified in [6])
(all other)		(reserved)	

6.4.7.3 Initialization Vector Length

Table 6.49: Initialization Vector Length Field

Field Name	Initialization Vector Length		
Definition	Length of the Initialization Vector of the employed encryption algorithm.		
Code values	Field Length [bits]	Value Range [decimal]	Description
	5	$1 \leq \text{length} \leq 31$	The length of the Initialization Vector is specified in terms of an integer, non-zero number of Bytes.
		0	Forbidden

6.4.7.4 Initialization Vector

Table 6.50: Initialization Vector Field

Field Name	Initialization Vector		
Definition	Initialization Vector defined by the employed encryption algorithm.		
Code values	Field Length [bits]	Value Range	Description
	As specified by the "Initialization Vector Length" parameter	Any value of the specified length	The Initialization Vector as defined by the encryption algorithm employed.

6.4.7.5 Block Size

Table 6.51: Block Size Field

Field Name	Block Size		
Definition	Size of the block the encryption algorithm operates on (in Bytes).		
Code values	Field Length [bits]	Value Range [decimal]	Description
	5	$1 \leq \text{length} \leq 31$	The Block Size is specified in terms of an integer, non-zero number of Bytes.
		0	Forbidden

6.4.7.6 Number of Padding Bytes

Table 6.52: Number of Padding Bytes Field

Field Name	Number of Padding Bytes		
Definition	Number of Padding Bytes required to obtain equal-size blocks for the encryption algorithm operations.		
Code values	Field Length [bits]	Value Range [decimal]	Description
	5	$0 \leq \text{length} \leq 31$	The Number of Padding Bytes is specified in terms of an integer number of Bytes.

6.4.8 Fields of the Alert Message Header

6.4.8.1 Alert Message Type

Table 6.53: Alert Message Type Field

Field Name	Alert Message Type		
Definition	Alert Protocol type or the type of data of the Alert Protocol Message (contained in the Payload) this specific AMH refers to.		
Code values	The defined code values identify the supported types of Alert Protocols the first release of the MAMES Protocol.		
	Field Length [bits]	Value Range [decimal]	Description
	5	0	Bulk (it includes: all the Alert Protocols currently not supported by MAMES and the case when no information regarding the Alert Protocol Message type is given).
		1	CAP. It includes: all CAP defined versions (as specified in [7] and [8]); CAP-XML, CAP-JSON, CAP-ASN.1 encoded CAP versions; all the defined CAP message types (Alert, Update, Ack, Cancel, Error).
		2	POCSAG message formats.
		3	A4A protocol (under development) [i.7].
		range of values mapped on the Internet Media Type ($4 \leq \text{type} \leq 13$)	Internet Media Types list. Details are reported in clause B.3.2.
(all other)		(reserved)	

NOTE: CAP and A4A Alert Protocols may contain also active content (e.g.: http links), that should be interpreted by the Alerting Devices. All other defined Alert Message Types should avoid any active content.

6.4.8.2 Language ID

Table 6.54: Language ID Field

Field Name	Language ID		
Definition	Identifier of the language of the corresponding Alert Protocol Message.		
Code values	The considered languages are the ones listed in clause B.3.1.		
	Field Length [bits]	Value Range [decimal]	Description
	8	0	language not specified
		$1 \leq ID \leq 183$	183 code values. The MAMES <Language ID> values are reported in clause B.3.1.
		(all other)	(reserved).

NOTE: The field value "0" is used e.g. in case no specific language knowledge is needed to understand the contents of the Alert Protocol Message (e.g. for images), or multiple languages are contained in the Alert Message.

6.4.8.3 Alert Message Length

The size of the whole MAMES Messages shall be smaller than, or equal to, the maximum allowed size of the SDU of the layer immediately below MAMES.

NOTE: The MAMES Alert Provider is aware of the maximum frame size allowed by the underlying layer.

Table 6.55: Alert Message Length Field

Field Name	Alert Message Length		
Definition	Length of the pertaining Alert Protocol Message (in Bytes)		
Code values	The code values are represented by the number of Bytes (binary encoded) of the length of the Alert Protocol Message, the AMH refers to. 24 bits allow a maximum Alert Protocol Message size of ~16 MB.		
	Field Length [bits]	Value Range [decimal]	Description
	24	1	AM length = 1 Byte
		2	AM length = 2 Bytes
	
		16777216	Maximum AM length ~16 MByte

6.4.8.4 More AMHs Flag

Table 6.56: More AMHs Flag Field

Field Name	More AMHs Flag		
Definition	Flag denoting if an AMH follows/does not follow the specific AMH.		
Code values	Field Length [bits]	Value Range [binary]	Description
	1	0	No more AMHs follow.
		1	At least one AMH follows.

7 Behaviour of MAMES Agents

7.1 Identification of a Set of behaviours

The objective of this clause is to introduce the description of the behavior of the MAMES Agents. The identified set of behaviors is provided in Table 7.1: for each MAMES Network entities the behaviours are listed, highlighting the specific event that occurs, the interested link (forward/return) and the involved processes of the MAMES Agents.

Table 7.1: MAMES Behaviour: MAMES Alert Provider and Receiver Actions

MAMES Network Entity	Link (forward/return)	Behaviour	Involved MAMES Process of the MAMES Agent	Process - Notes
MAMES Alert Provider	forward	Actions of MAMES Provider upon reception of an Alert Protocol Message from an Alert Issuer.	MAMES Composition	Composition of: MAMES ALERT, Ultra-short MAMES ALERT, MAMES UPDATE and MAMES CANCEL.
		Actions of MAMES Provider for declaring a valid MAMES Message obsolete (MAMES errors handling).		
	return	Actions of MAMES Provider upon reception of a MAMES ACK from a MAMES Receiver.	MAMES ACK Parsing	-
MAMES Alert Receiver	forward and return	Actions of MAMES Receiver upon reception of a MAMES Frame (ALERT, Ultra-Short ALERT, UPDATE, CANCEL).	MAMES Parsing	Parsing of: MAMES ALERT, Ultra-short MAMES ALERT, MAMES UPDATE and MAMES CANCEL.
			MAMES ACK Composition	-
	return	Actions of MAMES Receiver upon reception of an Alert Acknowledgment from Alerting Device.	MAMES ACK Composition	-

NOTE: MAMES ACK Composition process is considered only if a MAMES ACK is requested. In detail it depends on the value of the *ACK Request Indicator* field of the MH of the received MAMES Frame.

In the following the listed behaviours are described and in particular the actions of the MAMES Alert Provider and Receiver are reported.

In the provided analysis:

- i) the main focus is on the operations performed by the MAMES Alerter and User-Side Agents, which are responsible for the MAMES protocol process;
- ii) the MAMES Messages composition and parsing processes are assumed to be performed in compliance with the defined MAMES Header fields (reported in clause 6.4);
- iii) an error-free channel (between the MAMES Alert Provider and the MAMES Alert Receiver) and error-free behavior of the agents are assumed.

7.2 MAMES Alert Provider Actions

7.2.1 Actions of MAMES Provider upon reception of an Alert Message from Alert Issuer (MAMES Composition Process)

Upon reception of one or more Alert Messages from the Alert Issuer, the MAMES Provider starts the MAMES Composition Process performed by the MAMES Alerter-Side Agent. In detail it:

- selects the MAMES Frame the Alert Message(s) shall be encapsulated in (MAMES ALERT, MAMES UPDATE) based on the indications received from the Alert Issuer:
 - MAMES ALERT shall be selected if AM(s) that refer to a particular aspect of an event needs to be transmitted for the first time over a Notification Area and if a specific Alert Protocol layer message type needs to be transmitted (e.g. CAP cancel, CAP update, CAP error, etc.).
 - MAMES UPDATE shall be selected if an update of a previously sent MAMES Message needs to be transmitted. This includes the case when an Alert Issuer wants to cancel or update an Alert Message formatted according to an Alert Protocol that does not include a mean to identify an Alert Message as a cancellation and an update message (basic Alert Protocol).

- (*only in critical network context*) Ultra-short MAMES ALERT shall be selected as a MAMES Frame, although a MAMES ALERT or UPDATE should have been sent. In this case the received Alert Message will not be transmitted due to the unavailability of network resources: the Ultra-short MAMES ALERT will be generated and transmitted.
- sets the fields of the MAMES Header of the selected MAMES Message type. The different headers fields are set, including:
 - the fields of the Mandatory Header of the selected MAMES Message type.
 - (*only for MAMES ALERT and UPDATE*) the fields of the EHs (if any) based on the indications received from the Alert Issuer;
 - (*only for MAMES ALERT and UPDATE*) the fields of the AMH(s) for each of the AMs that need to be encapsulated in the MAMES payload.
- generates the MAMES Frame: composition of the MAMES Header and MAMES Payload, containing the encapsulated Alert Protocol Messages (if any).
- sends the MAMES Frame to the appropriate queue for transmission over the MAMES Alert Provider associated network. The queue selection shall be based on the value of the *MAMES Transport Priority* field of the MAMES MH.
- (*only for MAMES ALERT and UPDATE*) acts according to the value of the *ACK Request Indicator* field of the MAMES MH:
 - if a MAMES ACK is not requested (*ACK Request Indicator* field value is "0") the MAMES Composition process is terminated.
 - otherwise a timer is set (including a timeout):
 - upon reception of a MAMES ACK referring to the previous transmitted MAMES Frame the timer is reset and the MAMES Composition process is terminated. The actions upon reception of a MAMES ACK are described in clause 7.2.3.
 - if the timeout is reached the timer is reset and the MAMES Composition process is terminated; since a MAMES ACK request is seen as a "delivery report request", no actions of the MAMES Alert Provider are associated to a missed reception of a MAMES ACK.

7.2.2 Actions of MAMES Provider for declaring a previous transmitted MAMES Frame obsolete (MAMES Composition Process)

To handle MAMES errors and notify the MAMES Alert Receiver that a previous sent MAMES Message shall be considered obsolete and shall not be forwarded to Alerting Devices anymore, the MAMES Alert Provider shall generate and issue a MAMES CANCEL. The CANCEL message shall refer to the MAMES Message that needs to be declared as obsolete.

Erroneous transmission of a MAMES Message due to human/machine error, unauthorized transmission, incorrect formatting represent some of the events that trigger the MAMES Alert Provider to start the MAMES Composition process for a MAMES CANCEL. In detail it:

- selects the MAMES CANCEL as the MAMES Frame to be generated;
- sets the fields of the MAMES CANCEL Header, including:
 - the fields of the CANCEL Mandatory Header;
 - the fields of the EHs (if any) as required;
- generates the MAMES CANCEL: MAMES CANCEL Header composition;
- sends the MAMES CANCEL to the appropriate queue for transmission over the MAMES Alert Provider associated network. The queue selection shall be based on the value of the MAMES Transport Priority field of the MAMES CANCEL MH;

- acts according to the value of the *ACK Request Indicator* field of the MAMES CANCEL MH:
 - if a MAMES ACK is not requested (*ACK Request Indicator* field value is "0") the MAMES Composition process is terminated;
 - otherwise a timer is set (including a timeout):
 - upon reception of a MAMES ACK referring to the previous transmitted MAMES Frame the timer is reset and the MAMES Composition process is terminated. The actions upon reception of a MAMES ACK are described in clause 7.2.3;
 - if the timeout is reached the timer is reset and the MAMES Composition process is terminated.

7.2.3 Actions of MAMES Provider upon reception of a MAMES ACK from MAMES Receiver (ACK Parsing Process)

Upon reception of a MAMES ACK from the MAMES Alert Receiver, the MAMES Alert Provider starts the MAMES ACK Parsing Process, performed by the MAMES Alerter-Side Agent. In detail it:

- **(only if the MAMES ACK contains a payload)** MAMES ACK Parsing. This involves:
 - the parsing of the MAMES ACK Header, including the MH, the EHs (if any) and the AMHs;
 - the decapsulation of the Alert Messages contained in the MAMES Payload according to the corresponding information carried by the AMHs;
 - the transmission of the decapsulated Alert Messages back to the Alert Issuer for successful notification of the reception of the transmitted Alert Messages. This action represents the termination of the MAMES ACK Parsing process;
 - the notification of the successful reception of the MAMES Message, the MAMES ACK refers to. In particular this information is used to properly terminate the MAMES Composition Process (timer reset), described in clause 7.2.1;
- **(only if the MAMES ACK does NOT contain a payload)** MAMES ACK Header parsing. This involves:
 - the parsing of the MAMES ACK Header, including the MH, the EHs (if any);
 - the notification of the successful reception of the MAMES Message, the MAMES ACK refers to. In particular this information is used to properly terminate the MAMES Composition Process (timer reset).

7.3 MAMES Alert Receiver Actions

7.3.1 Actions of MAMES Receiver upon reception of a MAMES Frame (Parsing Process and MAMES ACK Composition Process)

The MAMES Alert Receiver can receive the following types of MAMES Messages: MAMES ALERT, MAMES UPDATE, MAMES CANCEL and Ultra-short MAMES ALERT. These are all the MAMES Message types that can be transmitted in the forward link from the MAMES Alert Provider to the MAMES Alert Receiver. As better described in the following the MAMES Parsing process performed by the MAMES User-Side Agent is differentiated based on the presence or absence of a MAMES Payload, on the type of the received MAMES Frame and on a MAMES ACK request.

Upon reception of a MAMES Frame from the MAMES Alert Provider, the MAMES Alert Receiver starts the MAMES Parsing Process, performed by the MAMES User-Side Agent. In detail it:

- checks if the MAMES Frame shall be processed based on the *Notification Area* field of the MH.

If the *Notification Area* check is not passed the MAMES Frame is discarded.

The following actions will be performed only if the *Notification Area* check is passed.

- MAMES Message Parsing:
 - parsing of the MAMES Header, including the MH, the EHs (if any) and the AMHs (if any). This operation includes the check of those EHs that include further information regarding the intended destination of the MAMES Frame (e.g. the *Administrative Areas Header*, the *MAMES Alert Scope* field of the *Alert and Response Type Header*). If the EHs check is not passed the MAMES Frame is discarded, otherwise the MAMES parsing process goes on.

The following actions will be performed only if the EHs check is passed.

- **(only if the MAMES Frame contains a payload - MAMES ALERT or MAMES UPDATE case -):**
 - decapsulation of the Alert Messages contained in the MAMES Payload according to the corresponding information carried by the AMHs;
 - transmission of the results of the decoded values of the headers fields and the decapsulated Alert Messages to the Alerting Device for rendering purposes. If a MAMES ACK is not requested, this action represents the termination of the MAMES Parsing process;
- **(only if the MAMES Frame does NOT contain a payload - MAMES ALERT or MAMES UPDATE, or MAMES CANCEL or Ultra-short MAMES ALERT case -):**
 - transmission of the results of the decoded values of the headers fields to the Alerting Device for rendering purposes. If a MAMES ACK is not requested, this action represents the termination of the MAMES Parsing process;
- **(only if a MAMES ACK is requested - MAMES ALERT or MAMES UPDATE or MAMES CANCEL case) MAMES ACK generation:**
 - transmission of the required configuration parameters to start the MAMES ACK Composition Process for the generation of the MAMES ACK to be transmitted back to the MAMES Alert Provider. The parameters include all the values that needed to set the fields of the MAMES ACK Header (MH and EHs as required). This action represents the termination of the MAMES Parsing process. The generation of a MAMES ACK is performed by the MAMES ACK Composition process;
 - start of the MAMES ACK Composition Process. In detail it:
 - sets the fields of the Mandatory Header of the MAMES ACK Header according to the received configuration parameters (from the MAMES Parsing process);
 - sets the fields of the EHs (if any) based on the indications received from the MAMES Parsing Process;
 - composing the MAMES ACK Header;
 - sends the MAMES ACK to the appropriate queue for transmission back to the MAMES Alert Provider over the MAMES Alert Receiver associated network. The queue selection shall be based on the value of the *MAMES Transport Priority* field of the MAMES ACK MH;
- **(only if a MAMES ACK is NOT requested - MAMES ALERT or MAMES UPDATE or MAMES CANCEL case) MAMES Message ID storage.** In detail if the ACK Request Indicator of the received MAMES Frame is set to "0", the MAMES Alert Receiver is not allowed to return any MAMES ACK Messages, although Alert Protocol Message Acknowledgements coming from the Alerting Device need to be transmitted (see clause 7.3.2). Therefore the MAMES Alert Receiver shall maintain a list of Message IDs of those received MAMES Frames that do not ask for a MAMES ACK.

NOTE: The MAMES Alert Receiver may start the MAMES ACK Composition process only if a MAMES ACK is requested.

7.3.2 Actions of MAMES Receiver upon reception of an Alert acknowledgement from an Alerting Device (MAMES ACK Composition Process)

Upon reception of an acknowledgement at Alert Protocol layer from an Alerting Device, the MAMES Alert Receiver starts the MAMES ACK Composition Process, performed by the MAMES User-Side Agent. In detail it:

- checks if it is allowed to return a MAMES ACK referring to the MAMES Frame the Alerting Device asks for (*MAMES Message ID* check):
 - if the *Message ID* of the MAMES Frame the MAMES ACK refers to is one of those stored in the MAMES Alert Receiver list (see clause 7.1.2.1), the received Alert Protocol Message Acknowledgement is discarded and the MAMES ACK Composition Process is terminated;
 - otherwise the MAMES ACK Composition Process continues.

The following actions will be performed only if the *MAMES Message ID* check is passed.

- sets the fields of the MAMES ACK Header based on the indications received from the Alerting Device, including:
 - the fields of the MAMES ACK Mandatory Header;
 - the fields of the EHs (if any) based on the received indications;
 - the fields of the AMH pertaining to the AM (Alert Protocol acknowledgement) that needs to be encapsulated in the MAMES payload;
- generates the MAMES ACK Frame: composition of the MAMES ACK Header and MAMES ACK Payload, containing the encapsulated Alert Protocol acknowledgement;
- sends the MAMES ACK to the appropriate queue for transmission over the MAMES Alert Receiver associated network. The queue selection should be based on the value of the *MAMES Transport Priority* field of the MAMES MH.

NOTE: The MAMES Alert Provider follows the Alert Protocol level instructions (received from the Alert Issuer), including requests for Alert Protocol Messages Acknowledgements. However if it is not possible (e.g. due to the unavailability of return channel capacity), the MAMES Alert Provider sets the *ACK Request Indicator* to "0". Upon reception of a MAMES Frame with the *ACK Request Indicator* set to "0", the MAMES Alert Receiver will not return a MAMES ACK and will discard all the Alert Protocol Message Acknowledgements coming from the Alerting Devices and referring to that MAMES Frame.

Annex A (normative): MAMES Requirements

A.1 General Functional Requirements

The high-level functional requirements that form the basis for the present document are reported. The definition of the MAMES requirements comes from an analysis of existing alerting systems requirements [i.11] to [i.15]. In particular, the general functional requirements on the MAMES Protocol are specified in the following.

MAMES Protocol shall:

- support the delivery of Alert Protocol Messages conforming to an established Alert Protocol standard or specification (advanced Alert Protocol);
- support the delivery of Alert Protocol Messages conforming to a basic Alert Protocol (e.g.: unstructured text, audio data, digital images);
- support the delivery of Alert Protocol Messages containing unspecified Alert Protocol;
- be capable of encapsulating one or more Alert Protocol Messages;
- support an indication specifying the relative priority of MAMES Frames with respect to other MAMES Frames;
- support an option to extend the mandatory functionalities by additional functionalities designed to enhance or facilitate the transport of the MAMES Frame through the network;
- support an option to extend the mandatory functionalities by additional functionalities designed to further characterize the encapsulated message or to support its processing or rendering by the MAMES User-Side Agent;
- support an authentication mechanism to enable the MAMES User-Side Agent to verify the identity of the MAMES Alert Provider;
- support an integrity mechanism to enable the MAMES User-Side Agent to verify that the MAMES frame has not been altered in transit;
- support an encryption mechanism to enable the MAMES Alerter-Side Agent to restrict the access to the MAMES Payload to certain MAMES User-Side Agents (namely those with a decryption capability);
- carry acknowledgement messages if requested by the encapsulated Alert Protocol (if the underlying network supports a return channel);
- support MAMES ACK messages for the purpose of acknowledging the receipt of an encapsulated Alert Message;
- support MAMES Frames containing a MAMES Header only.

A.2 MAMES Alerter-Side Agent Requirements

The requirements on the MAMES Alerter-Side Agent are specified in the following:

- upon reception of an Alert Message from an Alert Issuer, the MAMES Alerter-Side Agent shall be capable of creating a MAMES Frame encapsulating the Alert Message;
- the MAMES Alerter-Side Agent shall be capable of encapsulating more than one Alert Message in a single MAMES Frame;
- when creating a MAMES Frame, the MAMES Alerter-Side Agent shall be capable of taking into account information contained in the Alert Message;

- the MAMES Alerter-Side Agent shall be capable of transmitting the MAMES Frame to an entity responsible for forwarding the MAMES Frame towards the MAMES User-Side Agents;
- the MAMES Alerter-Side Agent shall be capable of performing security-related operations on Alert Messages;
- the MAMES Alerter-Side Agent shall be capable of requesting a MAMES ACK Frame from a MAMES User-Side Agent to indicate that the MAMES User-Side Agent has successfully received a previous MAMES Frame;
- upon reception of a MAMES ACK Frame from a MAMES User-Side Agent, the MAMES Alerter-Side Agent shall forward the encapsulated Alert Protocol Messages (if any) to the intended destination (Alert Issuer);
- the MAMES Alerter-Side Agent shall be capable of creating a MAMES Frame containing a MAMES Header only.

A.3 MAMES User-Side Agent Requirements

The requirements on the MAMES User-Side Agent are specified in the following:

- upon reception of a MAMES Frame, the MAMES User-Side Agent shall parse the MAMES Header to determine whether the MAMES Frame shall be further processed or be discarded;
- after having accepted a MAMES Frame as relevant, the MAMES User-Side Agent shall perform decapsulation to produce the Alert Message(s) contained in the MAMES Payload (if any);
- upon completion of the decapsulation procedure, the MAMES User-Side Agent shall take into account the information contained in the MAMES Header while performing all subsequent actions;
- the MAMES User-Side Agent shall forward the Alert Message(s) resulting from decapsulation towards functional entities according to the information contained in the MAMES Header;
- upon reception of an Alert Protocol-specific acknowledgement message from an Alerting Device, the MAMES User-Side Agent shall be capable of encapsulating that message and forward the resulting MAMES ACK Frame towards the originating MAMES Alerter-Side Agent;
- upon reception of a MAMES Frame containing a request for a MAMES ACK Frame, the MAMES User-Side Agent shall be capable of generating a MAMES ACK Frame, which it shall send to the MAMES Alerter-Side Agent;
- upon reception of a MAMES Frame containing a MAMES Header only, the MAMES User-Side Agent shall generate an Alert Message according to the information contained in the MAMES Header, which it shall forward to functional entities responsible for transmission towards the Alerting Devices.

Annex B (normative): MAMES Frame Field Details

B.1 Mandatory Header Fields Details

B.1.1 Notification Area Field Details

Table B.1 reports the code values of the radius index of the Notification Area field.

Table B.1: Notification Area MH Field: Radius

Radius index=code value	log(radius[km])	radius[km]	rounded km-values	Meaning
0	-	-	-	radius unspecified
1	0	1,00	1	radius up to 1 km
2	0,25	1,78	2	radius up to 2 km
3	0,5	3,16	3	radius up to 3 km
4	0,75	5,62	6	radius up to 6 km
5	1	10,00	10	radius up to 10 km
6	1,25	17,78	20	radius up to 20 km
7	1,5	31,62	30	radius up to 30 km
8	1,75	56,23	60	radius up to 60 km
9	2	100,00	100	radius up to 100 km
10	2,25	177,83	200	radius up to 200 km
11	2,5	316,23	300	radius up to 300 km
12	2,75	562,34	600	radius up to 600 km
13	3	1 000,00	1 000	radius up to 1 000 km
14	3,25	1 778,28	2 000	radius up to 2 000 km
15	-	-	2 000	radius greater than 2 000 Km

B.2 Extension Header Fields Details

B.2.1 <Area IDs>: Administrative Area Codes Mapping

For each of the administrative area coding schemes (NUTS, LAU, ISO 3166-1 [i.6]), a table mapping the numeric indexes used for encoding the *Area IDs* field of the *Administrative Area Header* and the administrative area codes is provided. The size of the *Area IDs* field depends on the administrative area coding scheme and on the number of areas denoted by the *Number of Areas* field.

Table B.2: <Area IDs> - NUTS Codes Mapping

Administrative Area Coding Scheme: NUTS			
<Area IDs> Code values	Field Length [bits per ID]	Value Range [decimal]	Description
	11	1 ≤ ID ≤ 1853	1853 NUTS code values (level 1, 2 and 3). The <Area IDs> (for NUTS) contained in archive ts_103337v010101p0.zip which accompanies the present document shall apply
		(all other)	(reserved).

Table B.3: <Area IDs> - LAU Codes Mapping

Administrative Area Coding Scheme: LAU				
<Area IDs> Code values	For each of the 27 EU Member States a range of Area IDs is defined. The <Area IDs> (for LAU) contained in archive ts_103337v010101p0.zip which accompanies the present document shall apply			
	Field Length [bits per ID]	Value Range [decimal]	Description	
	17		1 ≤ ID ≤ 2357	AT LAU code values
			2358 ≤ ID ≤ 2946	BE LAU code values
			2947 ≤ ID ≤ 8248	BG LAU code values
			8249 ≤ ID ≤ 8863	CY LAU code values
			8864 ≤ ID ≤ 15113	CZ LAU code values
			15114 ≤ ID ≤ 26408	DE LAU code values
			26409 ≤ ID ≤ 28652	DK LAU code values
			28653 ≤ ID ≤ 28878	EE LAU code values
			28879 ≤ ID ≤ 35008	EL (GR) LAU code values
			35009 ≤ ID ≤ 43122	ES LAU code values
			43123 ≤ ID ≤ 43464	FI LAU code values
			43465 ≤ ID ≤ 80146	FR LAU code values
			80147 ≤ ID ≤ 83298	HU LAU code values
			83299 ≤ ID ≤ 86739	IE LAU code values
			86740 ≤ ID ≤ 94833	IT LAU code values
			94834 ≤ ID ≤ 95388	LT LAU code values
			95389 ≤ ID ≤ 95504	LU LAU code values
			95505 ≤ ID ≤ 95622	LV LAU code values
			95623 ≤ ID ≤ 95690	MT LAU code values
			95691 ≤ ID ≤ 96121	NL LAU code values
			96122 ≤ ID ≤ 98600	PL 2479 LAU code values
			98601 ≤ ID ≤ 102860	PT LAU code values
			102861 ≤ ID ≤ 106040	RO LAU code values
			106041 ≤ ID ≤ 106330	SE LAU code values
			106331 ≤ ID ≤ 106540	SI LAU code values
		106541 ≤ ID ≤ 109468	SK LAU code values	
		109469 ≤ ID ≤ 119778	UK LAU code values	
	(all other)	(reserved).		

Table B.4: <Area IDs> - ISO 3166 Codes Mapping

Administrative Area Coding Scheme: ISO 3166-1 [i.6]				
<Area IDs> Code values	The <Area IDs> (for ISO 3166-1 [i.6]) contained in archive ts_103337v010101p0.zip which accompanies the present document shall apply.			
	Field Length [bits per ID]	Value Range [decimal]	Description	
	10		1 ≤ ID ≤ 249	249 officially assigned ISO 3166-1 [i.6] codes
			250 ≤ ID ≤ 657	Other ISO 3166-1 [i.6] codes (Exceptionally reserved, Transitionally reserved, Indeterminately reserved, Formerly used and Unassigned).
		(all other)	(reserved).	

B.3 Alert Message Header Fields Details

B.3.1 <Language ID> Codes

Table B.5 reports a mapping between the considered languages [i.8] and the MAMES code values (in decimal). The <Language ID> field length is 8 bits.

Table B.5: < MAMES Language ID > Codes

MAMES Language ID allowed values (decimal)	English name of Language
1	Abkhazian
2	Afar
3	Afrikaans
4	Akan
6	Amharic
7	Arabic
8	Aragonese
10	Assamese
11	Avaric
12	Avestan
13	Aymara
14	Azerbaijani
15	Bambara
16	Bashkir
18	Belarusian
19	Bengali
20	Bihari languages
21	Bislama
23	Bosnian
24	Breton
25	Bulgarian
27	Catalan; Valencian
28	Central Khmer
29	Chamorro
30	Chechen
32	Chinese
33	Church Slavic; Old Slavonic; Church Slavonic; Old Bulgarian; Old Church Slavonic
35	Corsican
36	Cree
37	Croatian
38	Czech
39	Danish
40	Divehi; Dhivehi; Maldivian
41	Dutch; Flemish
43	English
44	Esperanto
45	Estonian
46	Ewe
47	Faroese
48	Fijian
49	Finnish
50	French
52	Gaelic; Scottish Gaelic
53	Galician
54	Ganda
55	Georgian
56	German
57	Greek, Modern (1453-)
58	Guarani
60	Haitian; Haitian Creole
61	Hausa
62	Hebrew
63	Herero
65	Hiri Motu
66	Hungarian
67	Icelandic
68	Ido
69	Igbo
70	Indonesian

MAMES Language ID allowed values (decimal)	English name of Language
71	Interlingua (International Auxiliary Language Association)
72	Interlingue; Occidental
73	Inuktitut
74	Inupiaq
75	Irish
76	Italian
77	Japanese
78	Javanese
79	Kalaallisut; Greenlandic
80	Kannada
81	Kanuri
82	Kashmiri
83	Kazakh
84	Kikuyu; Gikuyu
85	Kinyarwanda
86	Kirghiz; Kyrgyz
87	Komi
88	Kongo
89	Korean
90	Kuanyama; Kwanyama
91	Kurdish
93	Latin
94	Latvian
95	Limburgan; Limburger; Limburgish
96	Lingala
97	Lithuanian
98	Luba-Katanga
99	Luxembourgish; Letzeburgesch
100	Macedonian
101	Malagasy
102	Malay
103	Malayalam
104	Maltese
105	Manx
106	Maori
107	Marathi
108	Marshallese
109	Mongolian
110	Nauru
111	Navajo; Navaho
112	Ndebele, North; North Ndebele
113	Ndebele, South; South Ndebele
114	Ndonga
115	Nepali
116	Northern Sami
117	Norwegian
118	Norwegian Nynorsk; Nynorsk, Norwegian
119	Occitan (post 1500)
120	Ojibwa
121	Oriya
122	Oromo
124	Pali
125	Panjabi; Punjabi
126	Persian
127	Polish
128	Portuguese
129	Pushto; Pashto
130	Quechua
131	Romanian; Moldavian; Moldovan
132	Romansh
133	Rundi
134	Russian
135	Samoan

MAMES Language ID allowed values (decimal)	English name of Language
136	Sango
137	Sanskrit
138	Sardinian
139	Serbian
140	Shona
141	Sichuan Yi; Nuosu
142	Sindhi
143	Sinhala; Sinhalese
144	Slovak
145	Slovenian
146	Somali
147	Sotho, Southern
148	Spanish; Castilian
149	Sundanese
150	Swahili
151	Swati
152	Swedish
153	Tagalog
154	Tahitian
155	Tajik
156	Tamil
157	Tatar
158	Telugu
159	Thai
160	Tibetan
161	Tigrinya
162	Tonga (Tonga Islands)
163	Tsonga
164	Tswana
165	Turkish
166	Turkmen
167	Twi
168	Uighur; Uyghur
169	Ukrainian
170	Urdu
171	Uzbek
172	Venda
173	Vietnamese
174	Volapük
175	Walloon
176	Welsh
177	Western Frisian
178	Wolof
179	Xhosa
180	Yiddish
181	Yoruba
182	Zhuang; Chuang
183	Zulu

B.3.2 <Alert Message Type>: Internet Media Type Mapping

Table B.6 reports a mapping between the Internet Media Types [i.9], [i.10] and the MAMES <Alert Message Type> code values.

Table B.6: < Alert Message Type > - Internet Media Types Mapping

Alert Message Type code value [decimal]	Internet Media Type
4	application
5	audio
6	example
7	image
8	message
9	model
10	multipart
11	text
12	video
13	application

Annex C (informative): MAMES Frames Examples

C.1 MAMES ALERT Frame

Figure C.1 shows an example of a MAMES ALERT Frame. In detail all the defined EHs are included and three Alert Protocol Messages are encapsulated in the Payload. The reported legend is valid for all the provided MAMES Frame examples.

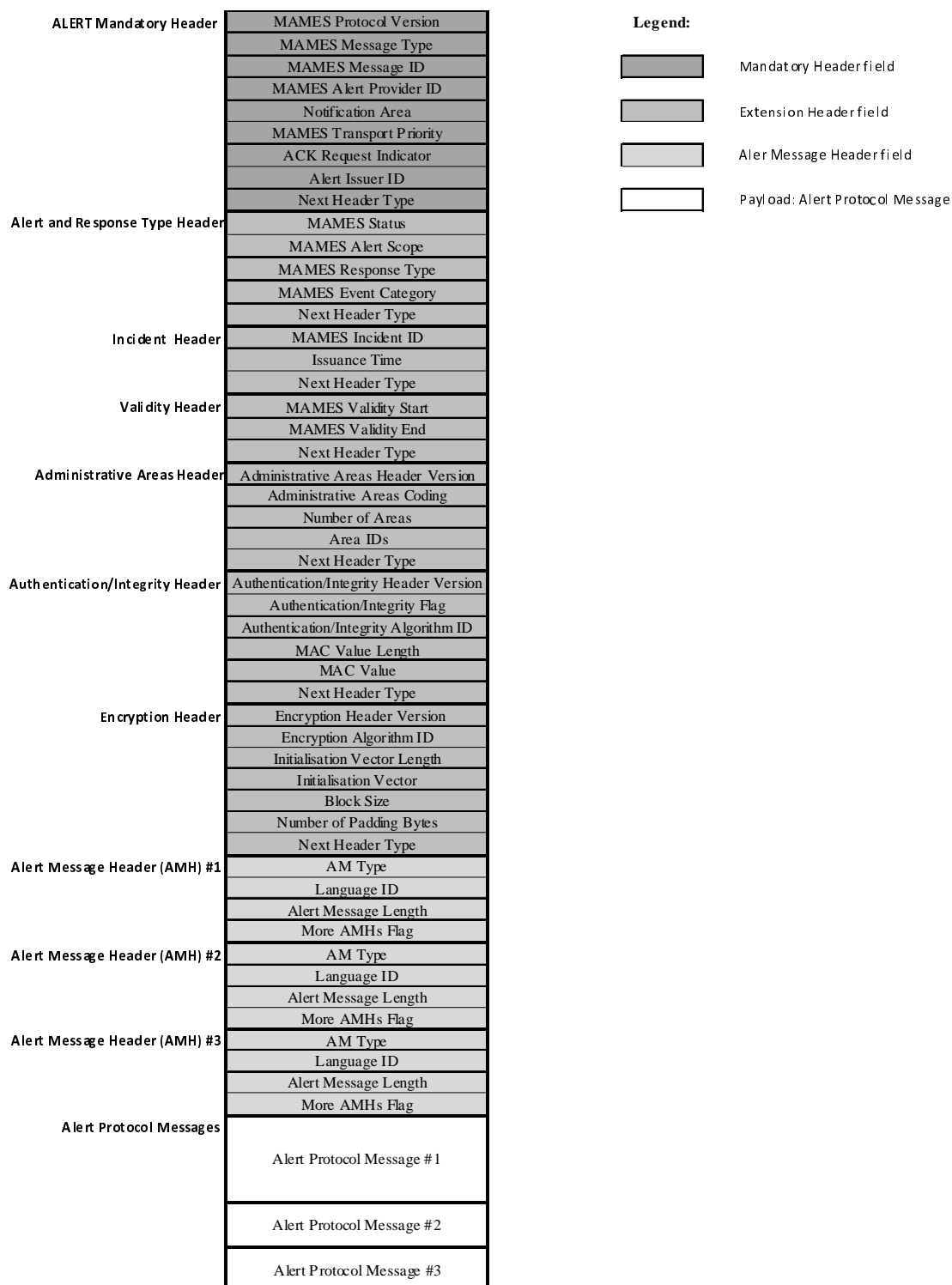


Figure C.1: MAMES ALERT Frame

C.2 MAMES Ultra-short ALERT Frame

Figure C.2 depicts an example of a MAMES Ultra-short ALERT Frame.

MAMES Protocol Version
MAMES Message Type
MAMES Message ID
MAMES Alert Provider ID
Notification Area
MAMES Transport Priority
Alert Issuer ID
MAMES Event Category

Figure C.2: MAMES Ultra-short ALERT Frame

C.3 MAMES UPDATE Frame

Figure C.3 depicts an example of a MAMES UPDATE Frame.

MAMES Protocol Version
MAMES Message Type
MAMES Message ID
MAMES Alert Provider ID
Notification Area
MAMES Transport Priority
MAMES Reference
ACK Request Indicator
Alert Issuer ID
Next Header Type
Updated Extension Headers
Alert Message Header(s) for updated Alert Message(s)
Corresponding updated Alert Message(s)

Figure C.3: MAMES UPDATE Frame

C.4 MAMES CANCEL Frame

Figure C.4 depicts an example of a MAMES CANCEL Frame.

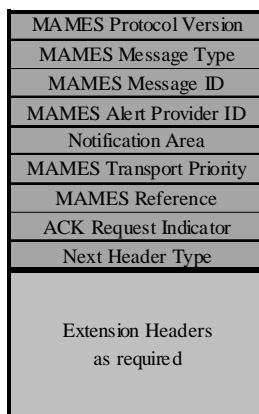


Figure C.4: MAMES CANCEL Frame

C.5 MAMES ACK Frame

Figure C.5 depicts an example of a MAMES ACK Frame.

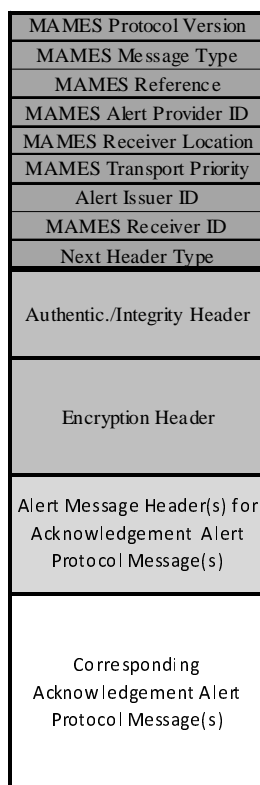


Figure C.5: MAMES ACK Frame

Annex D (normative): MAMES Headers Concatenation

D.1 Adopted Notation: Headers Fields Numbering

In order to describe the positioning of each field within the MAMES Headers, Table D.1 reports the field numbering only used for the purposes of this annex. All the MAMES Headers fields are listed together with an identification number. For completeness a column reporting the size of the field is reported.

Table D.1: Headers Fields Numbering

Field #	Field Name	Field Size [bits]
1	MAMES Protocol Version	4
2	MAMES Message Type	4
3	MAMES Message ID	12
4	MAMES Alert Provider	12
5	Notification Area	48
6	MAMES Transport Priority	2
7	ACK Request Indicator	1
8	Alert Issuer ID	16
9	Next Header Type	4
10	MAMES Event Category	4
11	MAMES Reference	12
12	MAMES Receiver Location	48
13	MAMES Receiver ID	16
14	MAMES Status	3
15	MAMES Alert Scope	3
16	MAMES Response Type	4
17	MAMES Incident ID	8
18	Issuance Time	32
19	MAMES Validity Start	32
20	MAMES Validity End	32
21	Administrative Areas Header Version	4
22	Administrative Areas Coding	4
23	Number of Areas	6
24	Area IDs	variable (maximum size 1 071 bits)
25	Authentication/Integrity Header Version	4
26	Authentication/Integrity Header Flag	1
27	Authentication/Integrity Header Algorithm ID	6
28	MAC Value Length	5
29	MAC Value	variable (maximum size 248 bits)
30	Encryption Header Version	4
31	Encryption Algorithm ID	6
32	Initialization Vector Length	5
33	Initialization Vector	variable (maximum size 248 bits)
34	Block Size	5
35	Number of Padding Bytes	5
36	AM Type	5
37	Language ID	8
38	Alert Message Length	24
39	More AMHs Flag	1

D.2 Mandatory Headers Fields Positioning

D.2.1 General Features

In order to introduce the *non-rotated* and *rotated* versions of the MAMES EHs and AMH, the MAMES Mandatory Headers of the defined MAMES Frames are shown, focusing on the positioning of each field within them.

All the defined MHs with the exception of the Ultra-short ALERT MH are 16 bits aligned for the applicability of the MAMES Headers concatenation algorithm.

Since no EHs and AMHs may be concatenated to the Ultra-short ALERT MH, the Ultra-short MAMES Frame shall not be aligned to 16 bits.

D.2.2 ALERT MH

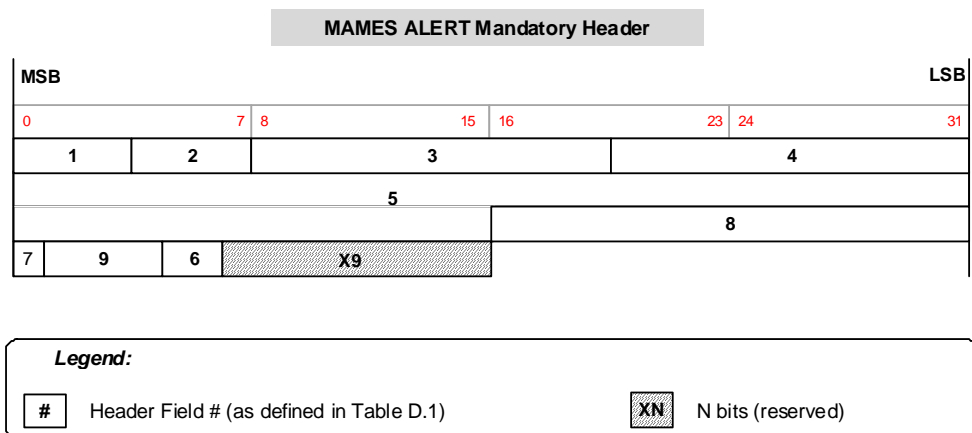


Figure D.1: ALERT MH Fields Positioning

D.2.3 Ultra-Short ALERT MH

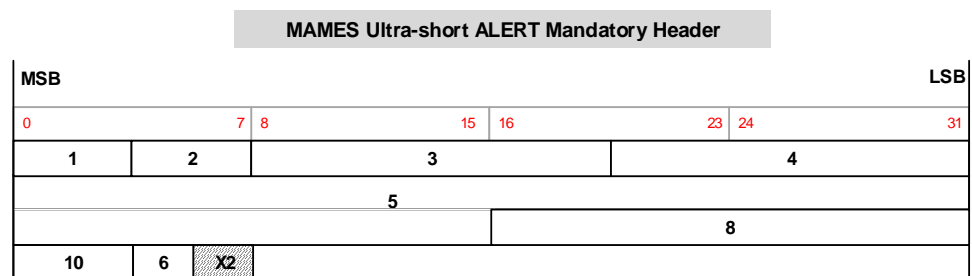


Figure D.2: Ultra-short ALERT MH Fields Positioning

D.2.4 UPDATE MH

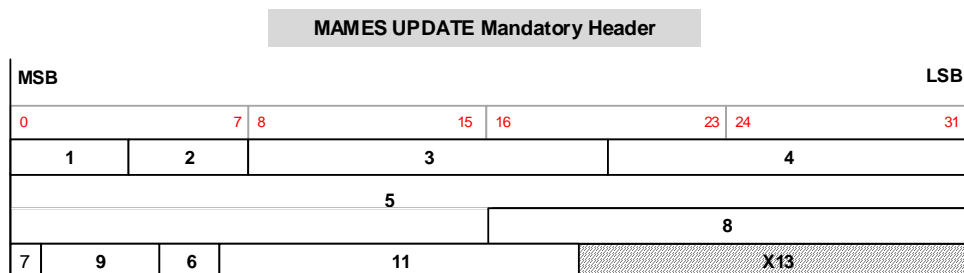


Figure D.3: UPDATE MH Fields Positioning

D.2.5 CANCEL MH

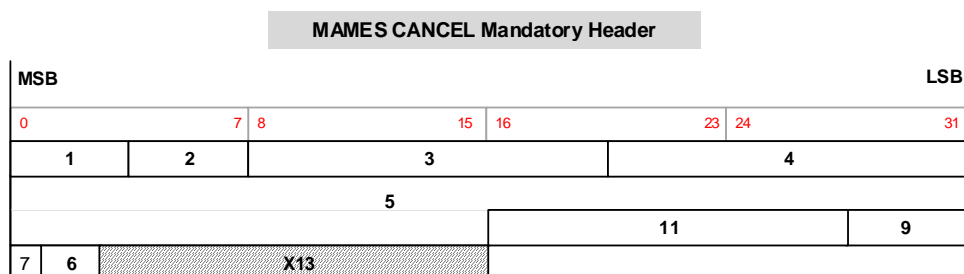


Figure D.4: CANCEL MH Fields Positioning

D.2.6 ACK MH

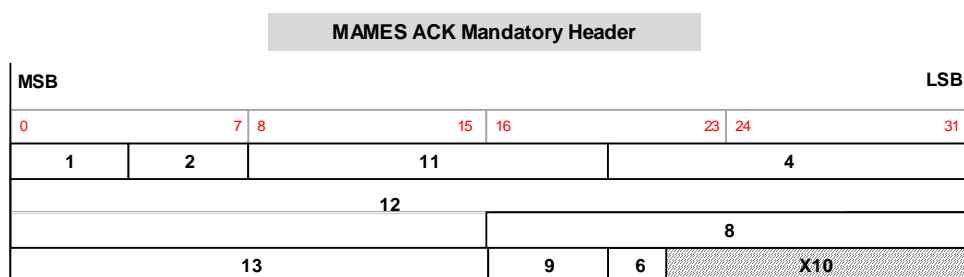


Figure D.5: ACK MH Fields Positioning

D.3 Extension Headers *non-rotated* and *rotated* Versions

D.3.1 General Features

The *non-rotated* and *rotated* versions of the MAMES EHs that shall be used for the composition of the MAMES Frame and in particular for the concatenation of the MAMES Headers according to the concatenation algorithm (clause 6.3.4) are defined. In detail the positioning of each field within each EH is provided.

D.3.2 Alert and Response Type Header

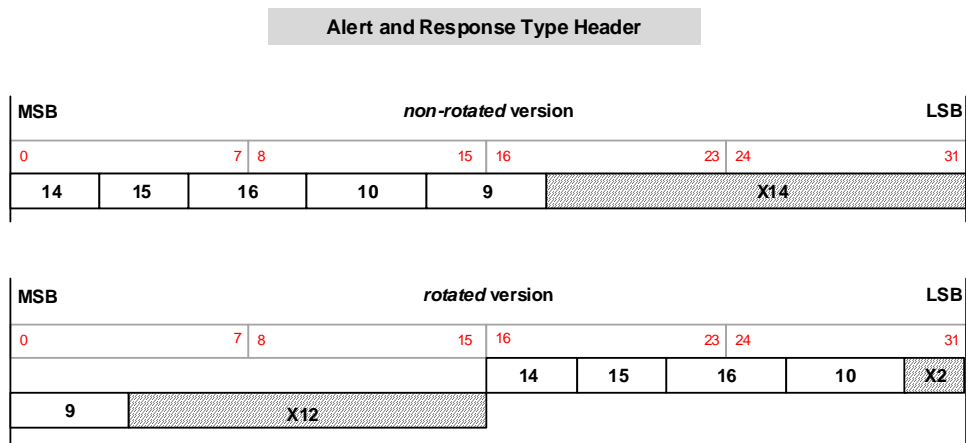


Figure D.6: Alert and Response Type Header non-rotated and rotated versions

D.3.3 Incident Header

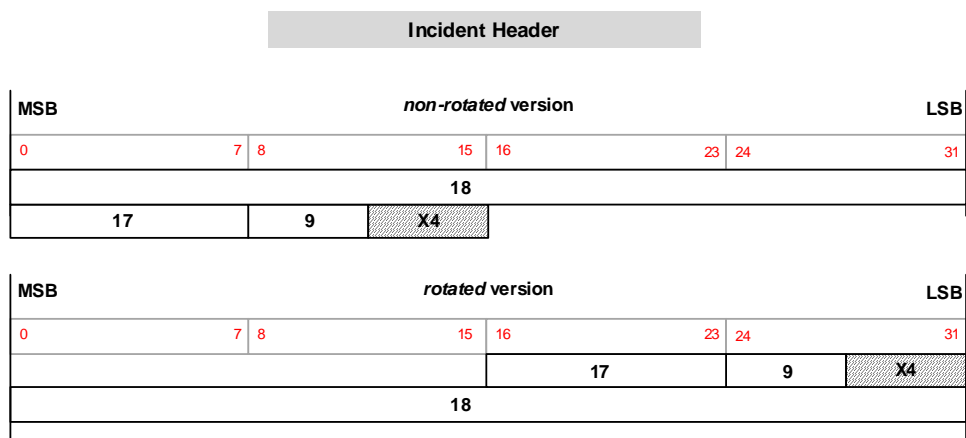


Figure D.7: Incident Header non-rotated and rotated versions

D.3.4 Validity Header

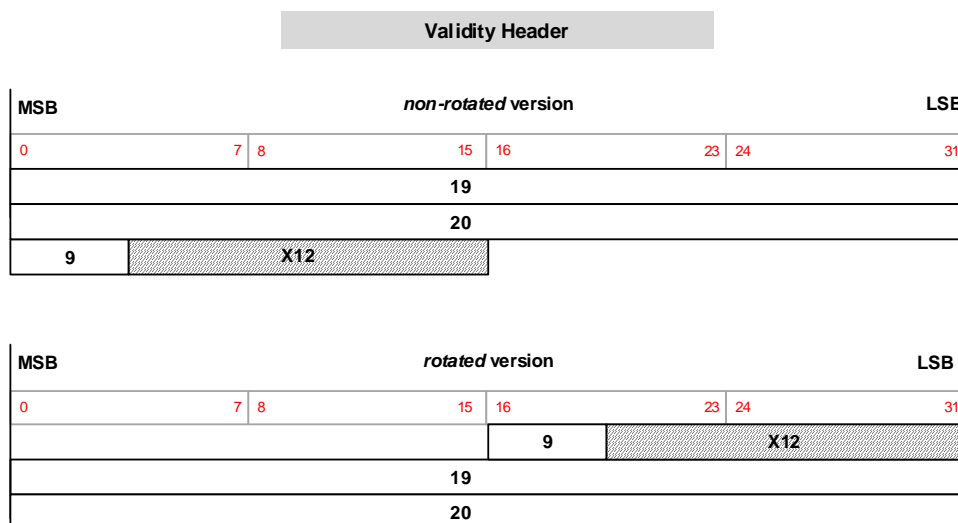


Figure D.8: Incident Header non-rotated and rotated versions

D.3.5 Administrative Areas Header

The Administrative Areas Header is of variable length. Its length depends on the length of the *Area IDs* field (numbered 24 in Figure D.9). As an example Figure D.9 reports the case of 5 areas and the adoption of NUTS Administrative Area coding scheme. This implies an *Area IDs* field of 55 bits.

The number of reserved bits depends on the effective length of this EH. In any case, as assumed in the description of the headers concatenation algorithm, 16-bit alignment shall be fulfilled. In the example depicted in Figure D.9, 5 reserved bits are used for 16-bit alignment (non-rotated version) and for 32-bit alignment (rotated version).

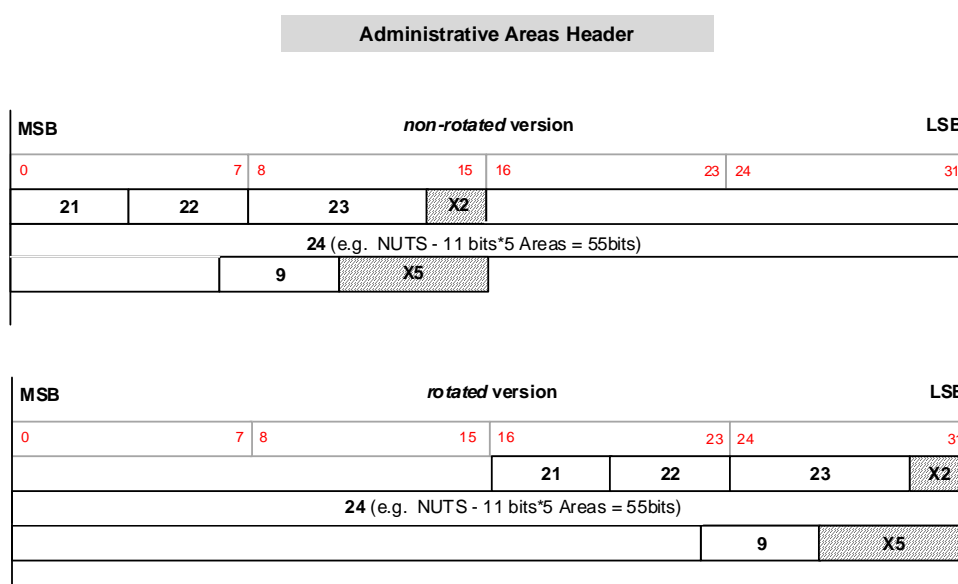


Figure D.9: Administrative Areas Header non-rotated and rotated versions

D.3.6 Authentication/Integrity Header

The Authentication/Integrity Header is of variable length. Its length depends on the length of the *MAC Value* field (numbered 29 in Figure D.10). As an example Figure D.10 reports the case of a MAC Value of 80 bits.

As for the Administrative Areas Header the number of reserved bits depends on the effective length of this EH.

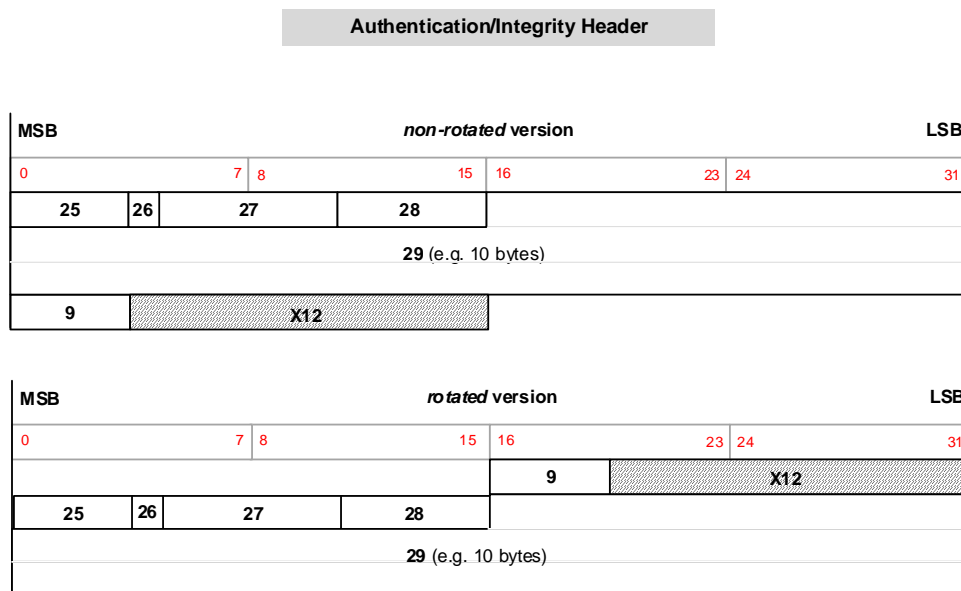


Figure D.10: Authentication/Integrity Header non-rotated and rotated versions

D.3.7 Encryption Header

The Encryption Header is of variable length. Its length depends on the length of the *Initialization Vector* field (numbered 33 in Figure D.11). As an example Figure D.11 reports the case of an Initialization Vector of 80 bits.

As for the Administrative Areas and Authentication/Integrity Headers, the number of reserved bits depends on the effective length of this EH.

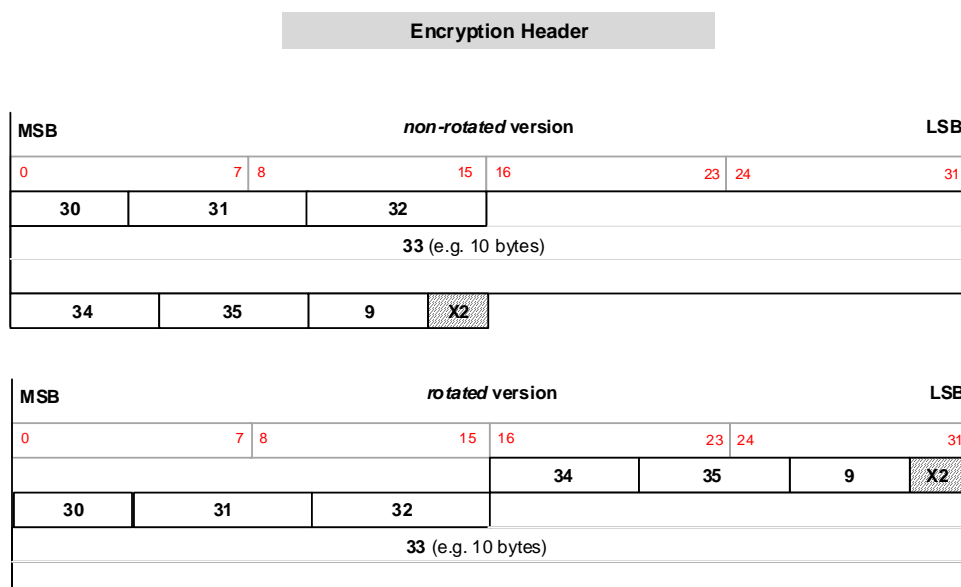


Figure D.11: Encryption Header non-rotated and rotated versions

D.4 Alert Message Header *Non-rotated* and *Rotated* Versions

The *non-rotated* and *rotated* versions of the MAMES Alert Message Header are defined in Figure D.12.

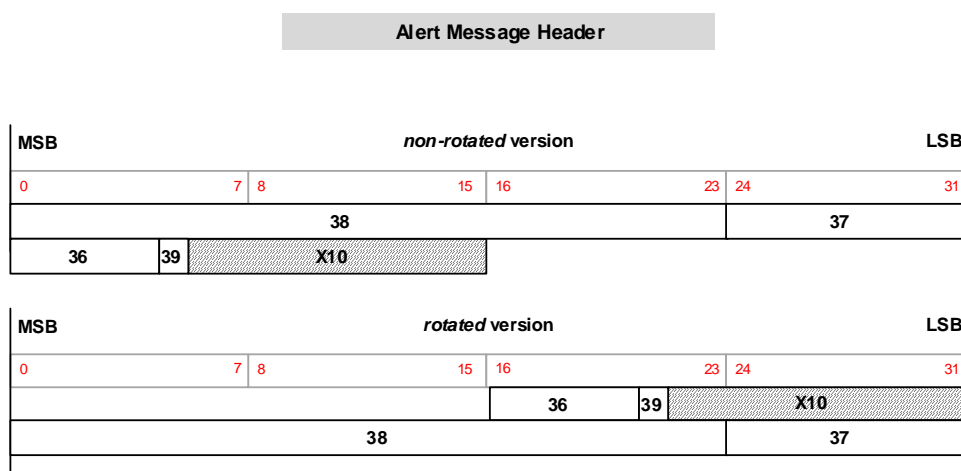


Figure D.12: Alert Message Header non-rotated and rotated versions

Annex E (informative): Description of the Behaviour of the MAMES Agents

E.1 Adopted Notation

As complementary information to the actions of the MAMES Alert Provider and Receiver analysed in clause 7, in the following a graphical representation of the essential behaviour of the MAMES Agents is provided. The adopted notation is introduced, the MAMES system together with its blocks is defined and finally the MAMES processes are detailed, providing a Finite State Machine diagram for each of them.

Figure E.1 depicts all the symbols used for the representation of the MAMES system and its components. While Table E.1 lists all the signals that are used in the definition of the MAMES Agents behaviour; in particular the adopted abbreviations are reported. The detail definition of these signals is out of the scope of the present document and depends on the implementation.

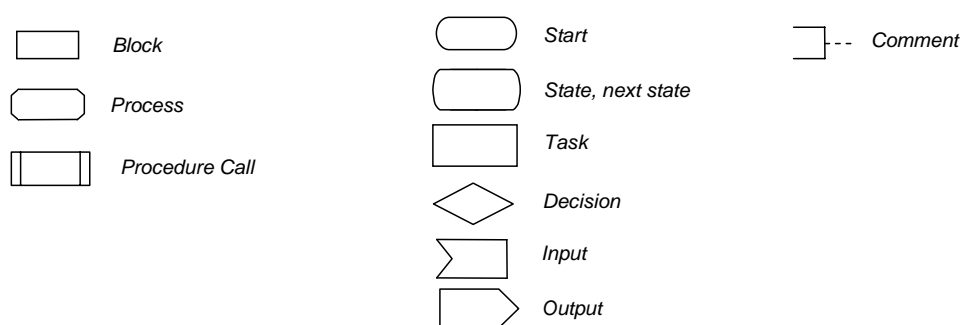


Figure E.1: Adopted Diagrams Symbols

Table E.1: Input/Output Signals: Adopted Notation and Abbreviations

Name	Abbreviation	Description
MAMES Message Forward Configuration Parameters	MFConfP	They include: all the required parameters for the MAMES Header generation (e.g.: parameters for MH, EHs and AMHs) and the AM(s) to be encapsulated in the MAMES Payload (if any).
MAMES ACK Configuration Parameters	MAckConfP	They include: all the required parameters for the MAMES ACK Header generation (e.g.: parameters for MH, EHs and AMHs) and the AM(s) to be encapsulated in the MAMES Payload (if any).
MAMES Forward Composition Output	MFCmpOut	It represents the result of the MAMES Composition process; it is the MAMES Frame forwarded to the MAMES Alert Receiver (MAMES User-Side Agent).
MAMES ACK Composition Out	MAckCompOut	It represents the result of the MAMES ACK Composition process; it is the MAMES ACK forwarded to the MAMES Alert Provider (MAMES Alerter-Side Agent).
MAMES ACK Reception notification	MAckRx	Notification of the reception of a MAMES ACK.
MAMES ACK Non-Reception notification	MAckNRx	Notification of the missed reception of a MAMES ACK.
MAMES Forward Frame Discarded	MFNOK	Notification of discard of the MAMES Frame (the MAMES Frame does not pass the check operations).
Alert Protocol Message Acknowledgement Discarded	AMAckNOK	Notification of discard of Alert Protocol Message Acknowledgement (the MAMES Frame the acknowledgement refers to does not request for an ACK).
MAMES Forward Parsing Output	MFParsOut	It includes: the decoded values of the MAMES Headers fields and the decapsulated AM(s) (if any), that are used by the Upper layers (of the Alerting Device) for rendering purposes.
Alert Protocol Message Acknowledgement	AMAck	It represents an Alert Protocol Message Acknowledgement coming from the Alerting Device.

E.2 MAMES System and MAMES Blocks

The MAMES system consists of two blocks: the MAMES Alerter-Side Agent and the MAMES User-Side Agent (as depicted in Figure E.2). It is worth highlighting that the only interface that is object of the present document is the one between the MAMES Agents (red arrows in the figure).

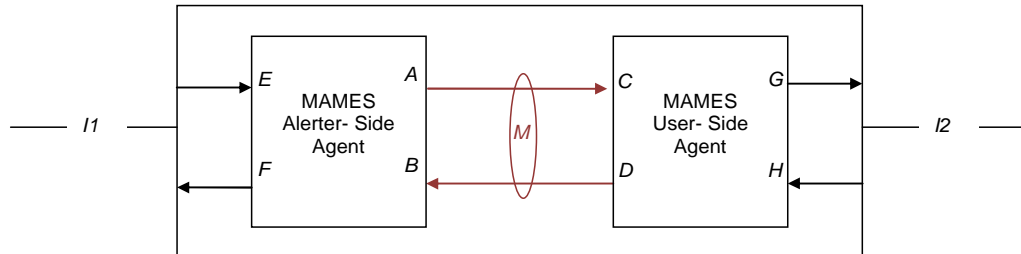


Figure E.2: MAMES System

Figure E.3 shows the MAMES Alerter-Side Agent block and its processes: MAMES Composition and MAMES ACK Parsing.

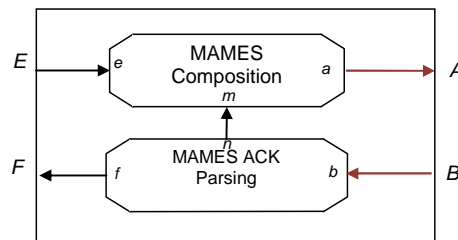


Figure E.3: MAMES Alerter-Side Agent Block

Figure E.4 shows the MAMES User-Side Agent block and its processes: MAMES Parsing and MAMES ACK Composition.

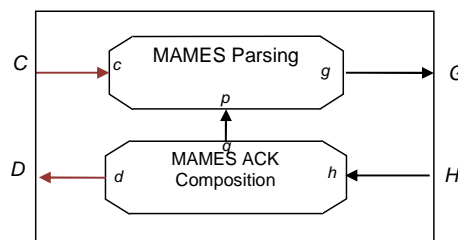


Figure E.4: MAMES User-Side Agent Block

E.3 MAMES Processes

E.3.1 Overview of the MAMES Processes and Corresponding Procedures

The behavior of the MAMES Agents is presented, providing a graphical representation of the finite state machine of the identified processes of the Agents. The descriptions of the MAMES processes given in the present annex assume:

- an error-free channel (between the MAMES Alerter-Side Agent and the User-Side Agent);
- an error-free behavior of the Agents;
- the generation of a MAMES ACK upon reception of a MAMES Frame that requests for a MAMES ACK (MAMES User Side Agent).

In order to introduce the processes representation, in Table E.2, for each of the defined block, an overview of the different processes and the corresponding procedures is reported. While the processes are described in the following clauses, no details are given on the procedures. The procedures operations, which may include messages, headers fields values local storage, are implementation dependent and therefore their definition is out of the scope of the present document.

Table E.2: Blocks, Processes and Procedures

Block	Process	Procedure	Notes
MAMES Alerter-Side Agent	MAMES Composition	MAMES Encapsulation	MAMES ALERT, UPDATE, CANCEL Frames composition.
		Ultra-short Composition	Ultra-short MAMES ALERT composition.
	MAMES ACK Parsing	MAMES ACK Decapsulation	It is applied to the MAMES ACK that contains a payload (decapsulation of Alert Protocol acknowledgement).
		MAMES ACK Header Parsing	It is applied to the MAMES ACK that does NOT contain a payload.
MAMES User-Side Agent	MAMES Parsing	Notification Area Check	Check of the Notification Area field of the MH to determine if the received MAMES Frame (MAMES ALERT, Ultra-short ALERT, UPDATE, CANCEL) is worth processing.
		MAMES Ultra-Short Header Parsing	It is applied to the Ultra-short MAMES ALERT.
		MAMES Header Parsing	It is applied to the MAMES Frame (ALERT, UPDATE, CANCEL) that does NOT contain a payload.
		MAMES Decapsulation	It is applied to the MAMES Frame (ALERT, UPDATE) that DOES contain a payload.
	MAMES ACK Composition	MAMES ACK Header Composition	Composition of MAMES ACK that does NOT contain a payload.
		MAMES ACK Encapsulation	Composition of MAMES ACK that DOES contain a payload (encapsulation of Alert Protocol acknowledgement).

E.3.2 MAMES Alerter-Side Agent Processes

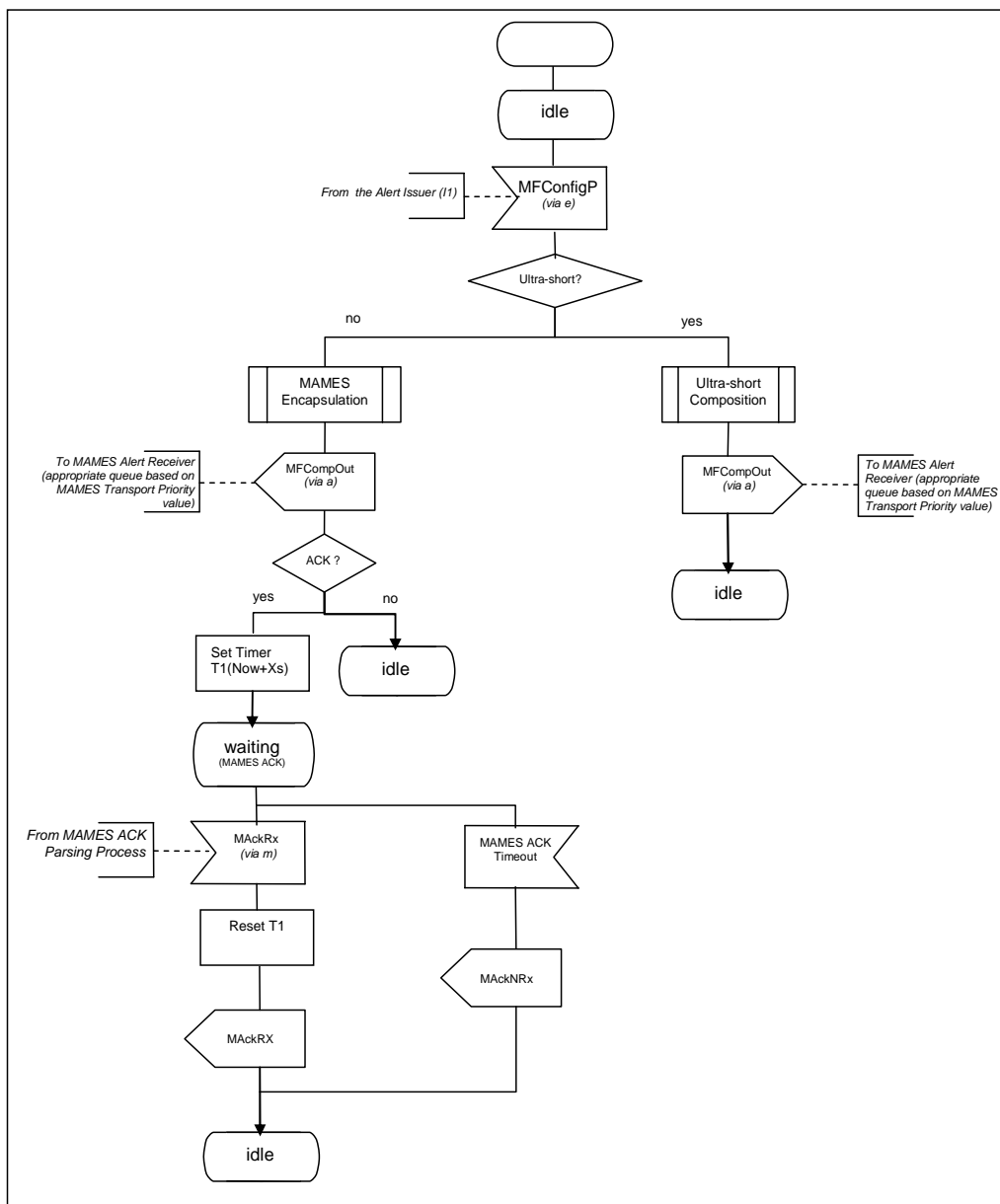


Figure E.5: MAMES Composition Process (MAMES Alerter-Side Agent)

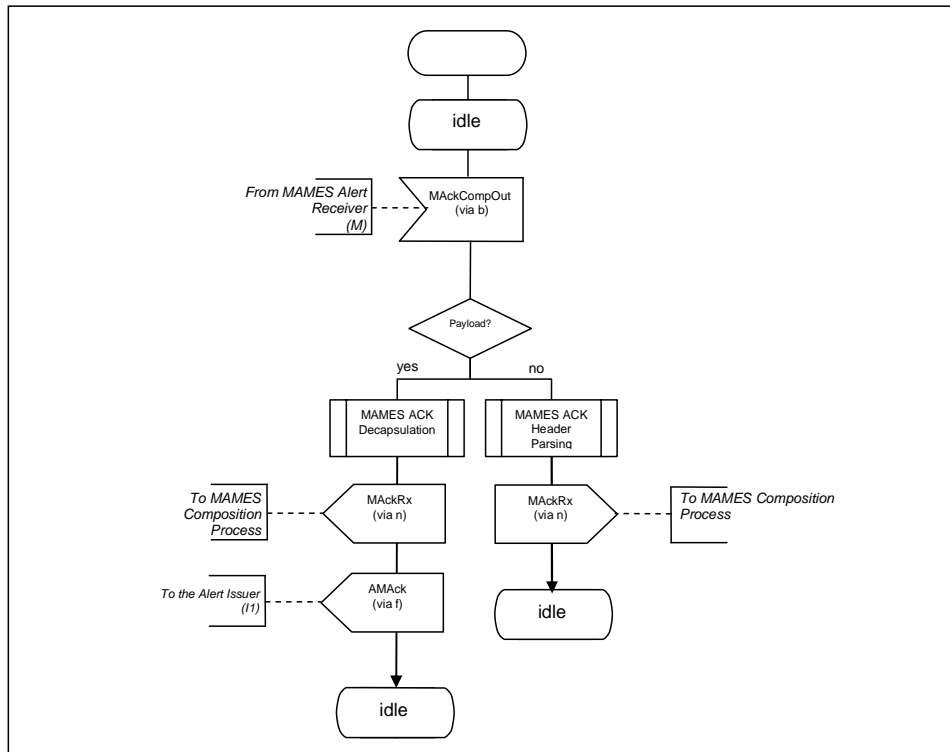


Figure E.6: MAMES ACK Parsing Process (MAMES Alerter-Side Agent)

E.3.3 MAMES User-Side Agent Processes

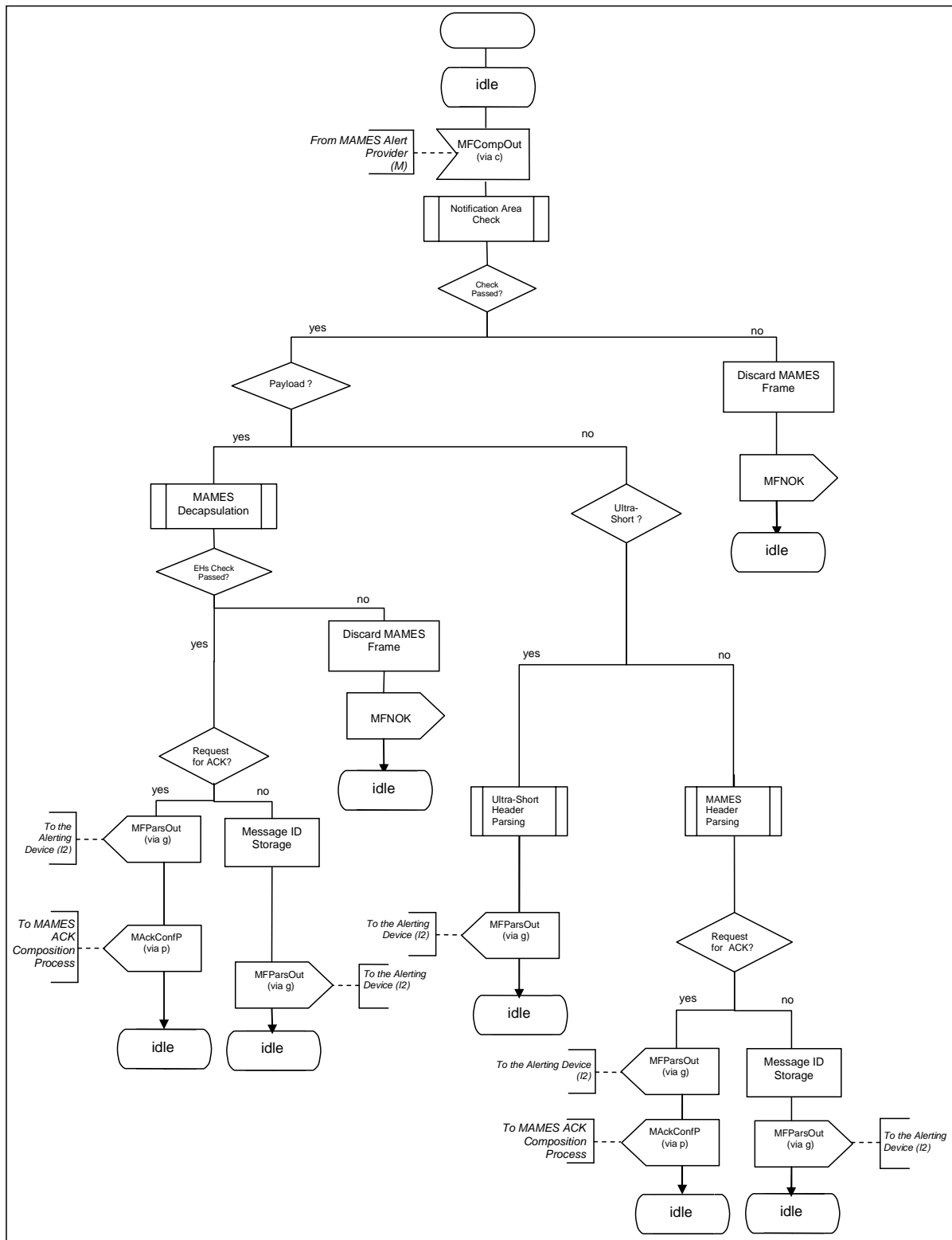


Figure E.7: MAMES Parsing Process (MAMES User-Side Agent)

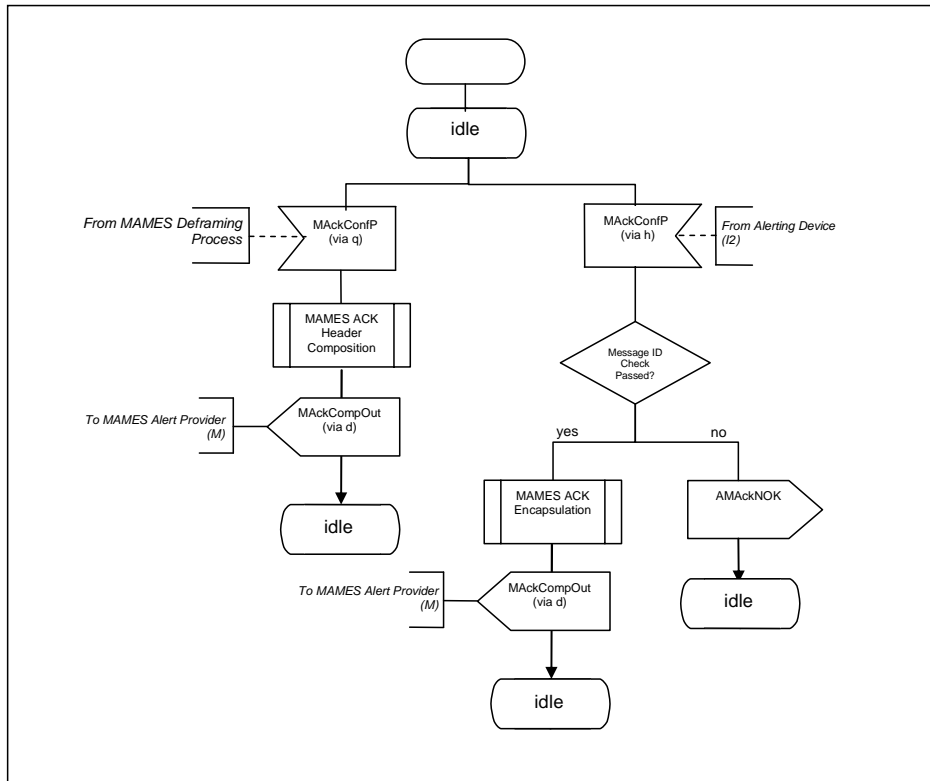


Figure E.8: MAMES ACK Composition Process (MAMES User-Side Agent)

History

Document history		
V1.1.1	May 2015	Publication