ETSI TR 118 546 V4.0.0 (2022-04)

oneM2M: Study on Public Warning Service Enabler (oneM2M TR-0046 v4.0.0 Release 4)

Reference
DTR/oneM2M-000046

Keywords
public safety, safety

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Partnership Project oneM2M (oneM2M).

1 Scope

The present document results of studies on public warning service enabler of oneM2M system. To enable public warning service over oneM2M system, the study includes following technical scope:

- Case studies of existing public warning systems.
- Use cases and potential requirements.
- Architecture analysis for the new use cases and requirements with current oneM2M system.
- Abstract data models for public warning services.

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.

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

Not applicable.

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] oneM2M Drafting Rules.

NOTE: Available at http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf.

[i.2] Recommendation ITU-T X.1303 bis: "Common alerting protocol (CAP 1.2)".

NOTE: Available at https://www.itu.int/rec/T-REC-X.1303bis-201403-I.

[i.3] oneM2M TS-0002 (Release 4):"Requirements".

[i.4] oneM2M TS-0023 (Release 4): "SDT based Information Model and Mapping for Vertical Industries".

[i.5] Home Gateway Initiative Smart Device Template.

NOTE: Available at https://git.onem2m.org/MAS/SDT/tree/master.

[i.6] ETSI TS 102 900: "Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service".

[i.7] IETF RFC 3066: "Tags for the Identification of Languages".

[i.8] IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[i.9] oneM2M TS-0001 (Release 4): "Functional Architecture".

[i.10] TTAK.OT-06.0054: "Common Alerting Protocol".

[i.11] TTAK.OT-06.0055: "Common Alerting Protocol Profile for Integrated Emergency Alert System".

[i.12] WGS84: "World Geodetic System 1984", International Civil Aviation Organization (ICAO).

[i.13] IETF RFC 7946: "The GeoJSON Format".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

EU-ALERT: generic term for the European Public Warning Service

Integrated Public Warning System (IPWS): integrated warning system that is operated by multiple authorities which can distribute messages to multiple communication channels

IPWS-M2M Interworking Proxy (IMIP): proxy that gets disaster messages from IPWS and send the translated message to M2M/IoT Service Platform

M2M Service Platform (MSP): M2M service platform that communicates with UDs and PDs in its M2M system

NL-ALERT: national variant of EU-ALERT for the Netherlands

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AE	Application Entity
API	Application Programming Interface
ASN	Application Service Node
BBK	Federal Office of Civil Protection and Disaster Assistance
CAP	Common Alerting Protocol
CBRNE	Chemical, Biological, Radiological, Nuclear or high-yield Explosive
CBS	Cell Broadcasting Service
CMAS	Commercial Mobile Alert System
CSE	Common Service Entity
DMB	Digital Multimedia Broadcasting
EAS	Emergency Alert System
EECC	European Electronics Communications Code
ETWS	Earthquake and Tsunami Warning System
EU	European Union
FEMA	Federal Emergency Management Agency
HGI	Home Gateway Initiative
HTML	Hyper Text Markup Language
IMIP	IPWS-M2M Interworking Proxy
IPAWS	Integrated Public Alert and Warning System
IPWS	Integrated Public Warning System
JITC	Joint Interoperability Test Command
LPWA	Low Power Wide Area
MN	Middle Node
MSP	M2M Service Platform
NAWAS	National Warning System
NOAA	National Oceanic and Atmospheric Administration
NWEM	Non-Weather Emergency Messages

NWR	NOAA Weather Radio
OSR	Overall System Requirements
PD	Public Device
PDT	Pacific Daylight Time
PEP	Primary Entry Point stations
PMO	Program Management Office
PWS	Public Warning System
RO	Read-Only
RW	Read/Write
SDT	Smart Device Template
SHA	Secure Hash Algorithm
TTA	Telecommunications Technology Association
TV	Television
UD	User Device
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USA	United States of America
WEA	Wireless Emergency Alert
WO	Write-Only
XML	Extensible Markup Language

4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

5 Case studies of existing public warning systems

5.1 Introduction

This clause contains several case studies for existing public warning systems, so that the relevant use cases and requirements, possibly, can be derived to specify the public warning service enabler over the oneM2M system. The interests to the case study is how public warning solutions can be extended for IoT systems, then warning information can also be consumed by things as well as human beings.

5.2 Public warning system in USA

In June 2006, after the Hurricane Katrina, it was initiated to integrate and modernize existing warning systems in the USA by the president's Executive Order 13407 including:

- Emergency Alert System (EAS)
- National Warning System (NAWAS)
- Commercial Mobile Alert System (CMAS)
- NOAA Weather Radio (NWR) All Hazards

The new warning system is an integrated system termed the Integrated Public Alert and Warning System (IPAWS). The IPAWS is the system deployed in the USA which is can be used by authorized officials to send out alerts to the public over multiple communication methods. Warning authorities are Federal, State, territorial, tribal and local which can send alert and warnings to their communities over multiple communication pathways including commercial mobile services, Internet services, National Weather Service, Emergency Alert System, state and local alerting systems.

Figure 5.2-1 shows the architecture combining standard alert message protocols, authenticated alert message senders, and shared access and distribution networks work together to deliver alerts and warnings through different communication pathways.

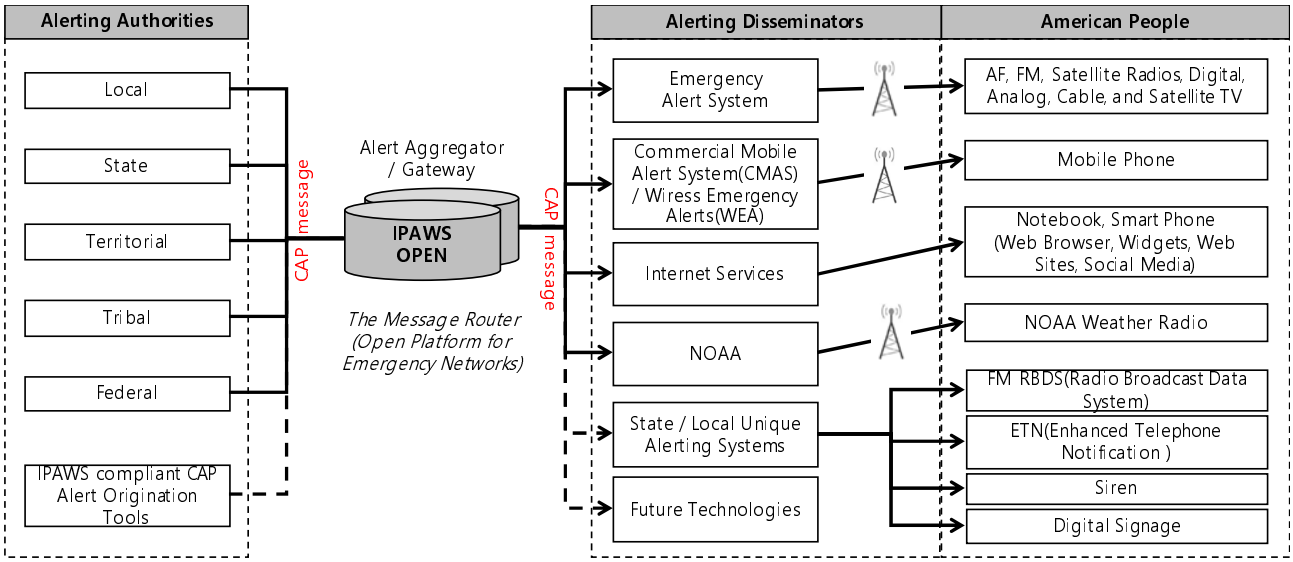


Figure 5.2-1: IPAWS Architecture

The IPAWS includes four components as below:

- Alerting systems
  - Emergency Alert System (EAS): the message dissemination pathway that sends warnings via broadcast, cable, satellite, and wireline services.
  - Wireless Emergency Alert (WEA): the message dissemination pathway that broadcasts alerts and warnings to cell phones and other mobile devices.
  - NOAA Weather Radio (NWR): a nationwide network of radio stations including 1 000 transmitters covering all 50 states, adjacent coastal waters, Puerto Rico, the U.S. Virgin Islands, and the U.S. Pacific Territories.
  - Internet Systems: the All-Hazards Emergency Message Collection System, also known as "HazCollect", automatically relays Non-Weather Emergency Messages (NWEM) over the internet to subscribing software providers.
- Protocol standards
  - Common Alerting Protocol (CAP): the digital format for exchanging emergency alerts that allows a consistent alert message to be disseminated simultaneously over many different communications systems.
  - IPAWS Profile: the standard for receipt and translation among devices intended to receive alerts from IPAWS.
- Infrastructure
  - Primary Entry Point stations (PEP): private or commercial radio broadcast stations that cooperatively participate with FEMA to provide emergency alert and warning information to the public before, during, and after incidents and disasters.
  - IPAWS Open Platform for Emergency Networks (IPAWS-OPEN): the Federal alert aggregator that receives and authenticates messages transmitted by alerting authorities and routes them to existing and emerging public alerting systems.
- Testing
  - IPAWS Supported State and Regional Tests: the IPAWS Program Management Office (PMO) supports efforts to improve IPAWS message delivery pathways and mitigate identified limitations by coordinating statewide and regional testing activities.

- Testing with the IPAWS Lab at JITC: the IPAWS PMO provides public safety officials with a controlled IPAWS testing environment where alert and warning technologies can be exercised to assess capabilities and effectiveness with IPAWS.

5.3 Public warning system in Europe

5.3.1 Standardization activities

All mobile phone users in Europe can receive public warning messages from any country in which they are currently located in. For this purpose, member states of the European Union provide a public warning system with their own regional requirements and regulations, while keeping compatibility with the EU-Alert technical specifications of the ETSI. The EU-Alert is a generic term for the European Public Warning Service based on 3GPP Cell Broadcast technology.

The Council of the European Union has adapted the new Directive on European Electronics Communications Code (EECC) to make all EU member states provide a public warning system. This system will send alerts to mobile phones that owned by all citizens and visitors who in a specific area in the event of emergencies. The due to implement of the public warning system is June 2022 for all EU members.

5.3.2 Public warning system in the Netherlands

The Dutch government provides a centralized national system for public warning service that informs emergencies to citizens through various channels such as the national siren system, social media and mobile phones.

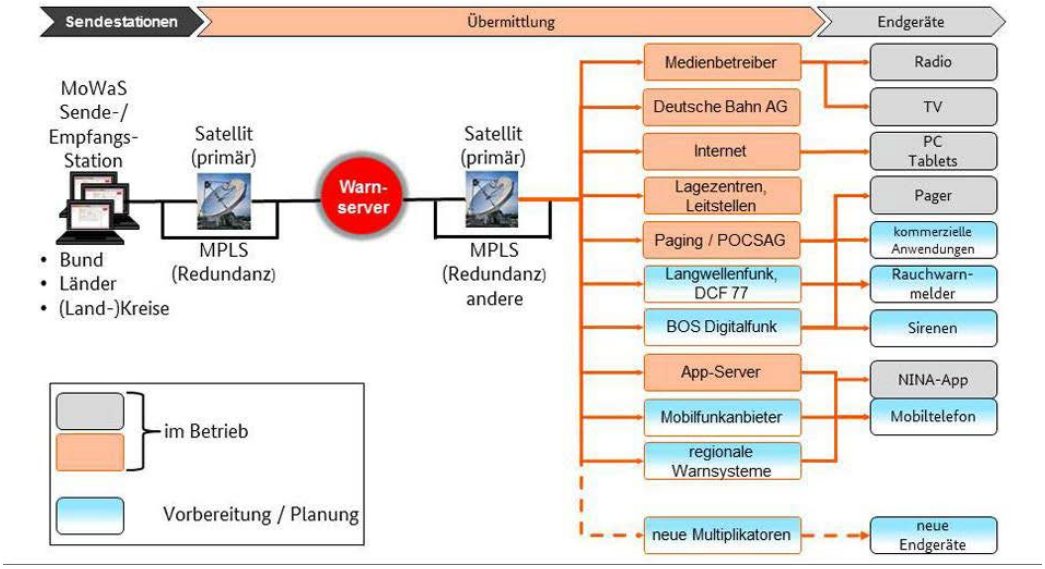
This system, introduced in 2012, is called NL-Alert. The NL-Alert is compliant with the EU-Alert (ETSI TS 102 900 [i.6]), so it is possible to receive warning messages via the cell phone even if the users are from other countries. The NL-Alert can also use more than 1 200 digital advertising screens in shopping centres, bus stops, trams and subways to display public warning messages for as many people as possible in the disaster area from June 2019.

5.3.3 Public warning system in Italy

Based on the two ministerial decrees in 2008 and 2011, the Common Alerting Protocol (CAP) became the standard document format for the exchange of emergency information in Italy. Since the first use of CAP message to exchange data between the Fire Corps and the Ministry for Cultural Heritage to coordinate their efforts in response activities to design and implement provisional measures for historical buildings during the 2009 Central Italy earthquake, CAP message is used to exchange emergency information between more than 100 provincial and regional control rooms and the national control centre in real time.

5.3.4 Public warning system in Germany

The German government provides the national Modular Warning System (MoWaS). It is designed to extend the classic warning communication channel (e.g. sirens) with new communication channels (e.g. smartphones, drones, responsive internet applications, etc.).



Source: BBK (German Federal Office of Civil Protection and Disaster Assistance; https://www.bbk.bund.de)

Figure 5.3.4-1: Structure of the Modular Warning System (MoWaS)

The MoWaS system divided into the three areas of trigger, transmission path and terminals. All the warning system blocks (e.g. smoke detector, mobile devices and apps) in these areas could be interwork through a common transmission protocol using the Common Alerting Protocol (CAP) as an open data format for the warning messages.

5.4 Public warning system in Korea

The public warning system in Korea is operated by the National Disaster and Safety Status Control Centre that is a division in the Ministry of the Interior and Safety. A main roll of the National Disaster and Safety Status Control Centre is to inform emergency situation to pubic through DMB (Digital Multimedia Broadcasting), CBS (Cell Broadcasting Service) and electric signages etc. In the case of disaster situation, the National Disaster and Safety Status Control Centre collects disaster information from related agencies to determine the severity, affected area and response activities. The determined information is used to disseminate warning message to public through digital broadcasting and text messages on mobile phone and electric signages.

The TTA has published two standards in 2014 and 2015 for the purpose to facilitate the exchange of disaster information between related agencies in response to disasters:

- TTAK.OT-06.0054 [i.10]
- TTAK.OT-06.0055 [i.11]

The first specification is developed by translating a referencing specification, the Common Alerting Protocol (CAP) version 1.2 [i.2] which is commonly used to exchange emergency information worldwide. The other specification defines additional requirements for implementation and operation of integrated public warning systems like civil defence alarm system.

Since the Korea has a high level of mobile phone penetration rate, the CBS is most important warning dissemination channel to inform emergencies to citizen. Figure 5.4-1 shows the pathway that the CBS warning message is delivered from authorities to mobile phone users.

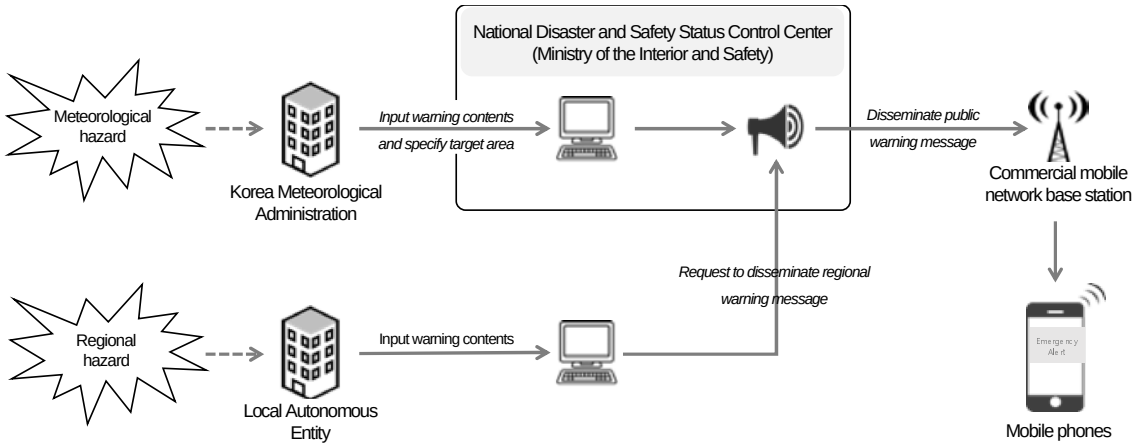


Figure 5.4-1: The procedure for dissemination of public warning message

5.5 Public warning system in Japan

5.5.1 J-ALERT

J-ALERT is the nationwide immediate alert system in Japan. After many operation tests, it was put into use in February 2007.

Its biggest feature is the concept of "Direct and immediate transmission from nation to citizen". To realize this, J-ALERT uses multiple communication methods; which are satellite, Local Government Wide Area Network, wired telephone network and area mailing service provided by mobile network operators.

Following kinds of information are notified with J-ALERT:

- Citizen protection information
  - Armed attack
  - Huge terrorism
  - Ballistic missile
- Disaster
  - Earthquake
  - Tsunami
  - Flood
  - Weather alert
  - Landslide
  - Tornado
  - Volcano

Figure 5.5.1-1 shows the Public Warning Systems in Japan architecture.

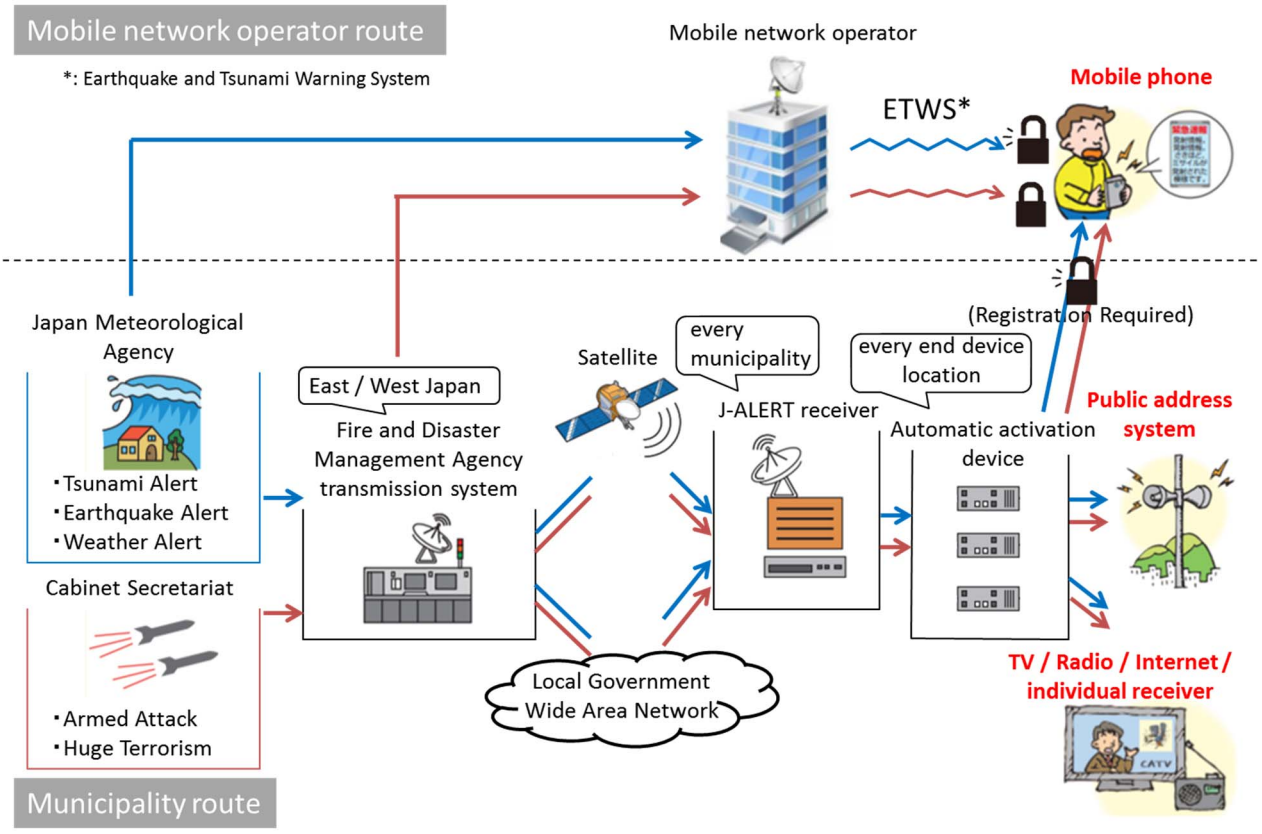


Figure 5.5.1-1: Public Warning Systems in Japan Architecture

When the disaster or matter of citizen protection occurs, Japan Meteorological Agency or Cabinet Secretariat sends the information to Fire and Disaster Management Agency transmission system at first. In case of the disaster, Japan Meteorological Agency sends to mobile network operators at the same time.

Second, Fire and Disaster Management Agency transmission system sends the information to J-ALERT receivers via both satellite and Local Government Wide Area Network , here the latter is used for backup purpose. In case of the matter of citizen protection, Fire and Disaster Management Agency transmission system sends to mobile network operators at the same time. There are two different routes as depicted in Figure 5.5.1-1; the mobile network operator route and the municipality route.

In the mobile network operator route, when mobile network operators gets information about the disaster or the matter of citizen protection, they directly and immediately sends these information to their users with Earthquake and Tsunami Warning System (ETWS). The detail about ETWS is described in clause 5.5.2.

In the municipality route, when J-ALERT receivers gets information about the disaster or the matter of citizen protection, they send these information to automatic activation devices.

Finally, automatic activation devices switch on end devices such as public address system, TVs, radios and Internet messages. This is the municipality route.

The number and location of each sending / receiving nodes are different. There are only two Fire and Disaster Management Agency transmission systems, the one covers East Japan and another covers West Japan. J-ALERT receivers are located at every municipalities and Automatic activate machines are located at every end device location.

The encrypted warning information used by J-ALERT can only be decoded by Japanese devices, but exceptionally, disaster information via mobile network operator route can be decoded every devices regardless of the nationality. When the matter of citizen protection occurs, a user of Non-Japanese device needs to register himself with his municipality to get the information on his mobile phone. As another option, Japanese Fire and Disaster Management Agency recommends installing some applications for notification.

5.5.2 ETWS

ETWS enable to broadcast disaster information immediately to all mobile phone users. The ETWS communication is given the best priority among other communications, this means ETWS communication is not easily affected by congestion. When sending message with ETWS, there is no need to specify addresses, but the confirmation of message arrival is not performed.

The origin of ETWS is Cell Broadcast Service (CBS) specified at 3GPP for broadcasting of Short Message Service. Next, because of a lot of demand for the disaster information delivery, 3GPP specified Public Warning System (PWS) based on CBS. PWS covers from 2G to Long Term Evolution (LTE).

The requirement for PWS varied from area to area. In USA, users wanted not only disaster but also crime and accident information. On the other hand, In Japan, users wanted immediacy for the alert for earthquake and tsunami. Then, Commercial Mobile Alert System (CMAS) was developed for the requirement from the former, and ETWS was developed for the requirement from the latter.

6 Use cases and potential requirements

6.1 Public warning service triggered by external system

6.1.1 Description

Background

- The USA, South Korea, Japan and some countries in Europe operate their own public warning systems to propagate warning and manage disastrous situations quickly and accurately.
- M2M/IoT systems which enables communications between machines or applications can play a pivotal role in this public warning systems while interworking with existing warning systems.

Description

- This is the use case of IoT/M2M enabled public warning service that is based on interworking between an existing integrated public warning system (IPWS) and an IoT/M2M system to transmit warning information to User Devices (UDs) and Public Devices (PDs) located in devastated area.
- In peace time, the UDs and the PDs do their programmed tasks, for example playing audio, locking door, lighting, displaying advertisement, etc. These UDs and PDs could work as safety assistive devices under emergency.
- Authorities invocate the IPWS to send out warning messages to citizens using the open API of the IPWS. Then the IPWS distributes warning messages through multiple channels including IoT/M2M systems. Finally, the IoT/M2M systems will propagate the warning messages to the UDs and the PDs in a high priority immediately.

6.1.2 Source

Void.

6.1.3 Actors

- Authorities: Public authorities that are responsible for warning citizens in emergency.
- Integrated Public Warning System (IPWS): Integrated warning system that is operated by multiple authorities which can distribute messages to multiple communication channels.
- IPWS-M2M Interworking Proxy (IMIP): Proxy that gets disaster messages from IPWS and send the translated message to M2M/IoT Service Platform.
- M2M Service Platform (MSP): M2M service platform that communicates with UDs and PDs in its M2M system.

- User Device (UD): Citizen-owned M2M/IoT devices which has safety assistive features in emergency.
- Public Device (PD): Public infrastructure M2M/IoT devices, owned by government or municipality, which has safety assistive features in emergency.

6.1.4 Pre-conditions

- IPWS uses Common Alerting Protocol (CAP) [i.2] which carries human understandable information.
- IMIP that gets warning messages from IPWS as human understandable information translates into machine understandable one, and send it to M2M/IoT system.
- Warning messages from IPWS can contain geo-location information on devastated areas so that a specific group of devices can get the warning.
- UDs and PDs understands the warning messages from the MSP so that reacts for emergency.

6.1.5 Triggers

An emergency situation occurs and the authority delivers the information to IPWS.

6.1.6 Normal Flow

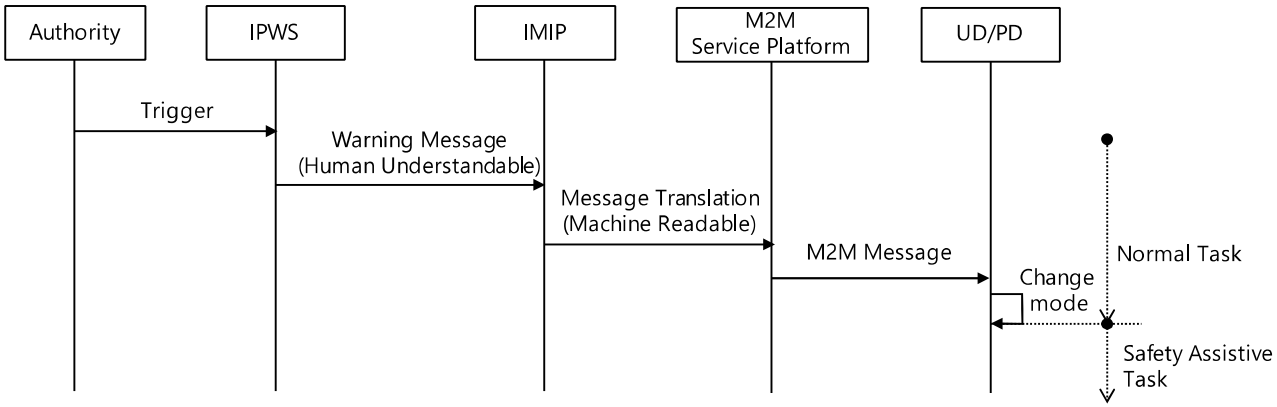


Figure 6.1.6-1: Use case Scenario Service Flow

1) Warning information triggered by authority is distributed to multiple channels including M2M/IoT system.
2) IMIP interprets the received IPWS warning into M2M/IoT message in public warning information model and send it to M2M Service Platform.
3) M2M Service Platform propagates the warning message to a group of UDs and PDs in specific geo-locations.
4) When the UDs and the PDs receives warning messages, they change the operation mode and work as safety assistive devices.

6.1.7 Alternative Flow

None.

6.1.8 Post-conditions

None.

6.1.9 High Level Illustration

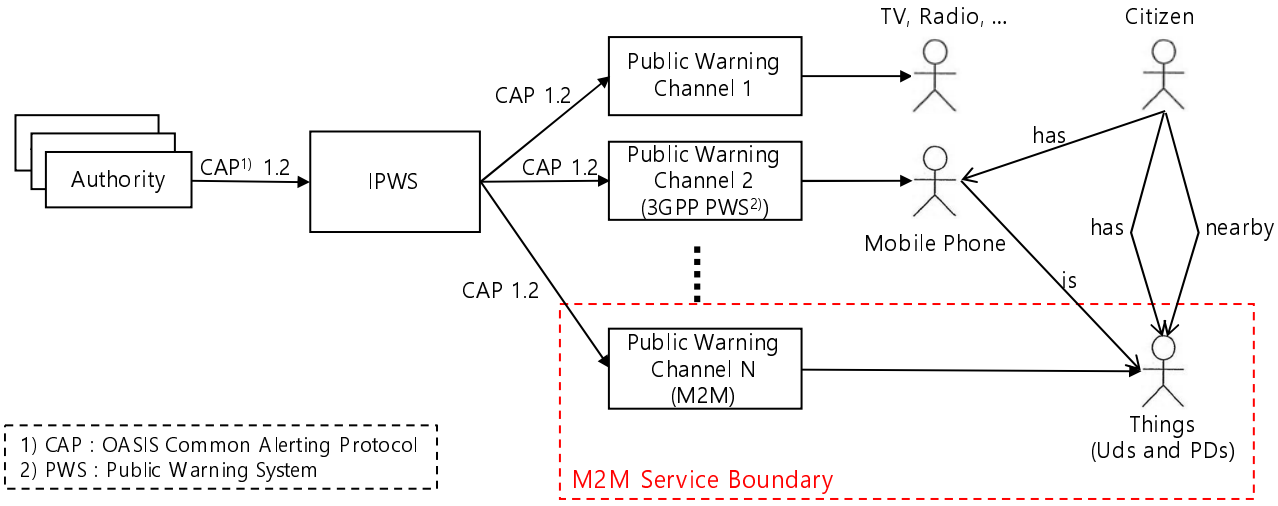


Figure 6.1.9-1: High level system view

6.1.10 Potential Requirements

This use case scenario can be fulfilled by the existing requirements as defined in oneM2M TS-0002 [i.3], (see Table 6.1.10-1).

Table 6.1.10-1: Related existing requirements as defined in oneM2M TS-0002 [i.3]

Requirement ID	Description	Release
OSR-094 See REQ-2015-0631R02	*The oneM2M System shall provide Information Model(s) to support interoperability among different devices/applications.*	*Implemented in Rel-2*
OSR-095 See REQ-2015-0631R02	*The oneM2M System should provide mappings between different Information Models from non-oneM2M System(s).*	*Not implemented*
OSR-096 See REQ-2015-0631R02	*The oneM2M System should be able to interwork with non-oneM2M System(s).*	*Implemented in Rel-2*
OSR-037	*The oneM2M System shall enable an M2M Application to request to send data, in a manner independent of the Underlying Network, to the M2M Applications of a group of M2M Devices and M2M Gateways in geographic areas that are specified by the M2M Application.*	*Not implemented*

The requirements in Table 6.1.10-2 can be considered as additional potential requirements for the use case in oneM2M TS-0002 [i.3].

Table 6.1.10-2: New potential requirement for oneM2M TS-0002 [i.3]

Requirement ID	Description
HLR-xxx	*The oneM2M System shall provide validation of geographic location information corresponding to supported formats.*

6.2 Enabling and disabling of public warning service

6.2.1 Description

Public warning service provides a means to public authorities to deliver warning messages to individuals in emergency. A widely used public warning service is based on the 3GPP Public Warning System (PWS) that sends text-based warning messages.

The use case described in this clause regards to the public warning service for M2M devices. While the 3GPP PWS makes the user aware of the emergency situation by using human-readable text-based warning messages through user's mobile phones and makes the user react by their decisions, in the public warning service over M2M/IoT Systems herein, M2M devices are performing pre-defined automated tasks (e.g. close gas valves) by themselves.

This use case also describes the M2M device side scenarios against warning notification for public warning service. In general, a public warning service is provided for the user's safety even if the user did not subscribe to the emergency service beforehand. So, a user who does not want the public warning service may disable the public warning service feature of his/her devices. On the other hand, depending on a criteria set by an authority, important notifications (e.g. earthquake, tsunami) need to be handled autonomously by the device as the authority intended, even if the user disabled the emergency service.

6.2.2 Source

None.

6.2.3 Actors

- Authority: is responsible for providing warning notification to citizens in emergency situations.
- M2M Service Platform (MSP): communicates with UDs and PDs in its M2M system.
- User Device (UD): is a Citizen-owned M2M/IoT device which performs pre-specified emergency tasks in emergency situations.
- Public Device (PD): is an M2M/IoT device in public infrastructures, owned by government or municipality, which performs pre-specified emergency tasks in emergency situations.
- User: is a person who owns UDs or who manages PDs.

6.2.4 Pre-conditions

- An UD or PD is already enabled for public warning service.
- An UD or PD performing its own normal tasks.

6.2.5 Triggers

- An authority generates a public warning notification in an emergency situation.

6.2.6 Normal Flow

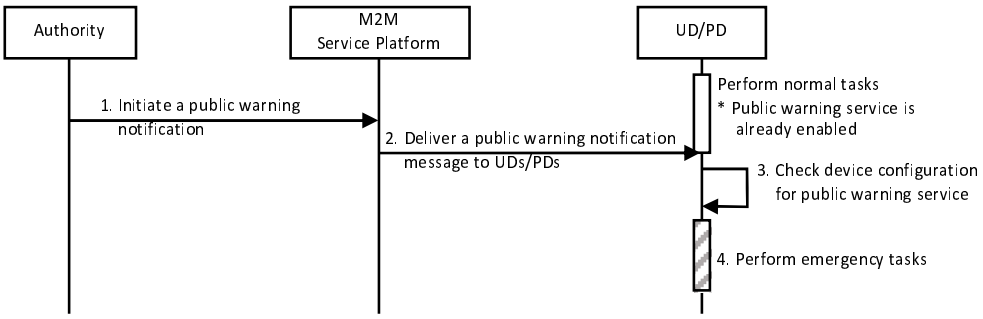


Figure 6.2.6-1: Normal flow for the public warning service enabled UDs/PDs

1) An authority generates a public warning notification and sends it to an M2M Service Platform.
2) The M2M Service Platform delivers the received public warning notification message to UDs/PDs.
3) The UD/PD checks its configuration (e.g. public warning service = enabled) whether the device needs to switch its mode into emergency mode.
4) The UD/PD performs emergency tasks when the public warning service is enabled.

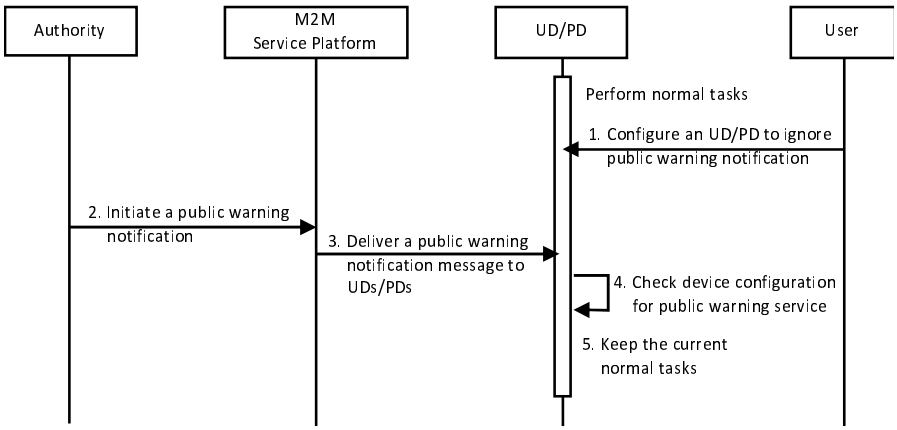


Figure 6.2.6-2: Normal flow for the public warning disabled UDs/PDs

1) A user changes the configuration of an UD/PD to ignore public warning notification.

2) An authority generates and sends a public warning notification.

3) An M2M Service Platform delivers the received public warning notification message to UDs/PDs.

4) The UD/PD checks its configuration (e.g. public warning service = enabled) whether the device needs to switch its mode into emergency mode.

5) The UD/PD keeps working on the normal tasks when the public warning service is disabled.

6.2.7 Alternative Flow

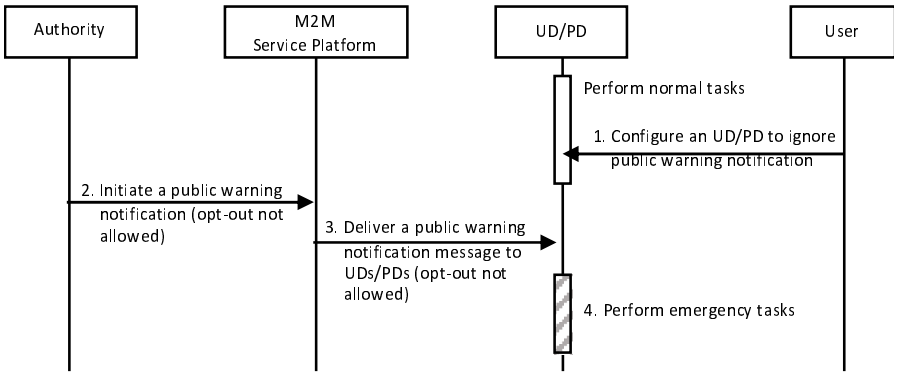


Figure 6.2.7-1: Alternative flow for the opt-out-not-allowed public warning notification

1) A user changes the configuration of an UD/PD to ignore public warning notification.

2) An authority generates and sends an opt-out-not-allowed public warning notification.

3) A M2M Service Platform delivers the received public warning notification message to UDs/PDs using M2M protocol.

4) If an opt-out-not-allowed public warning notification is received, then the UD/PD is enforced to perform emergency tasks even though the configuration for the public warning service is disabled.

6.2.8 Post-conditions

None.

6.2.9 High Level Illustration

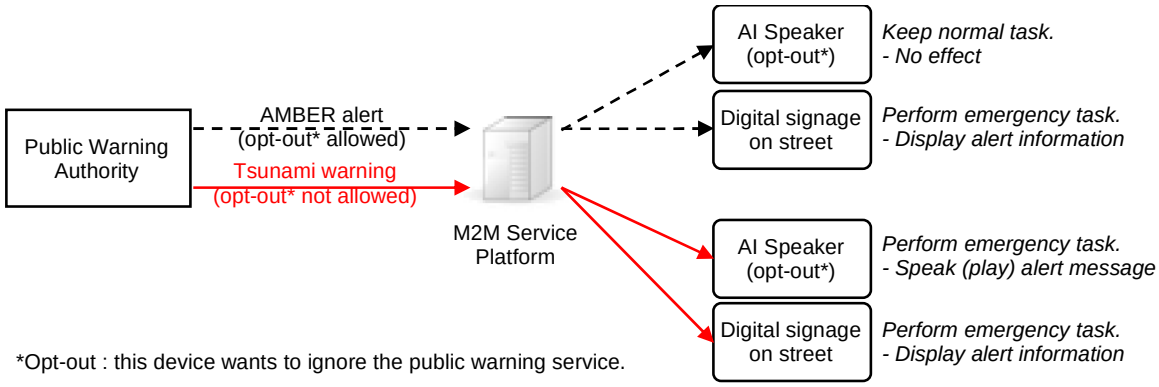


Figure 6.2.9-1: High level illustration of enabling and disabling public warning service

6.2.10 Potential Requirements

This use case scenario can be fulfilled by the existing requirements as defined in oneM2M TS-0002 [i.3], (see Table 6.2.10-1).

Table 6.2.10-1: Related existing requirements as defined in oneM2M TS-0002 [i.3]

Requirement ID	Description	Release
OSR-084 See REQ-2015-0595R04	*The oneM2M System shall be able to handle an event notification from an authorized M2M Application which triggers actions to be performed on the M2M Device* *EXAMPLE: Turn on or off the monitoring.*	*Not implemented*
MGR-001	*The oneM2M System shall be able to support management and configuration of M2M Gateways/ Devices including resource constrained M2M Devices.*	*Implemented in Rel-1*
MGR-019 See REQ-2015-0555R02	*The M2M Device shall be able to accept standardized configuration settings from an external configuration server in order to register to the oneM2M System.*	*Not implemented*
MGR-001	*The oneM2M System shall be able to support management and configuration of M2M Gateways/ Devices including resource constrained M2M Devices.*	*Implemented in Rel-1*

The requirements in Table 6.2.10-2 can be considered as additional potential requirements for the use case in oneM2M TS-0002 [i.3].

Table 6.2.10-2: New potential requirements for oneM2M TS-0002 [i.3]

Requirement ID	Description
HLR-xxx	*The oneM2M System shall support categorization of public warning notifications (e.g. 3GPP PWS Warning Messages).*
HLR-xxx	*The oneM2M System shall be able to support the opt-in or opt-out to public warning notifications by M2M Devices.*

6.3 Selective respond to emergency types

6.3.1 Description

IoT devices are in charge of a given simple task using limited computing resources. The emergency task that triggered by a public warning message is also a given simple task for specific emergency event (e.g. automatic control gas valve when receive earthquake warning). In other words, an IoT device responds to specific type of emergency event rather than all types of emergencies. M2M System may provide a mechanism to deliver public warning message to the device which interested in.

6.3.2 Source

None.

6.3.3 Actors

- Warning originator: Responsible for providing warning notification to citizens in emergency situation.
- M2M Service Platform (MSP): M2M service platform that communicates with UDs and PDs in its M2M system.
- Device: M2M/IoT devices which perform pre-defined emergency tasks in emergency situation.

6.3.4 Pre-conditions

- A device is configured to enable the public warning service.

6.3.5 Triggers

- A warning originator sends a warning message that contain emergency type.

6.3.6 Normal Flow

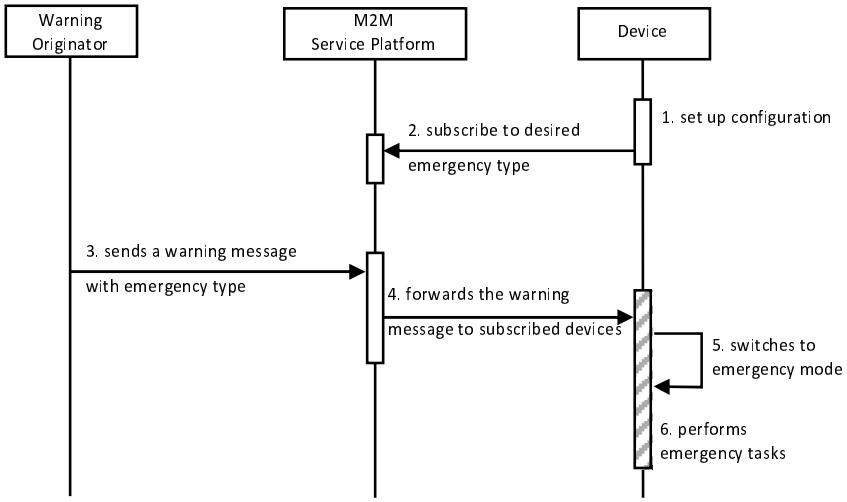


Figure 6.3.6-1: Normal flow for the selective respond to type of emergencies

1) A device setup configuration including types of emergencies which device interested in.
2) The device subscribe to receive emergency notification for designated types.
3) A warning originator sends a warning message including type of emergencies.
4) A M2M service platform forwards the received warning message to devices that subscribed on type of emergency event specified in warning message.
5) A device switches to emergency mode when a warning message is received.
6) A device performs emergency tasks that are pre-defined.

6.3.7 Alternative Flow

None.

6.3.8 Post-conditions

None.

6.3.9 High Level Illustration

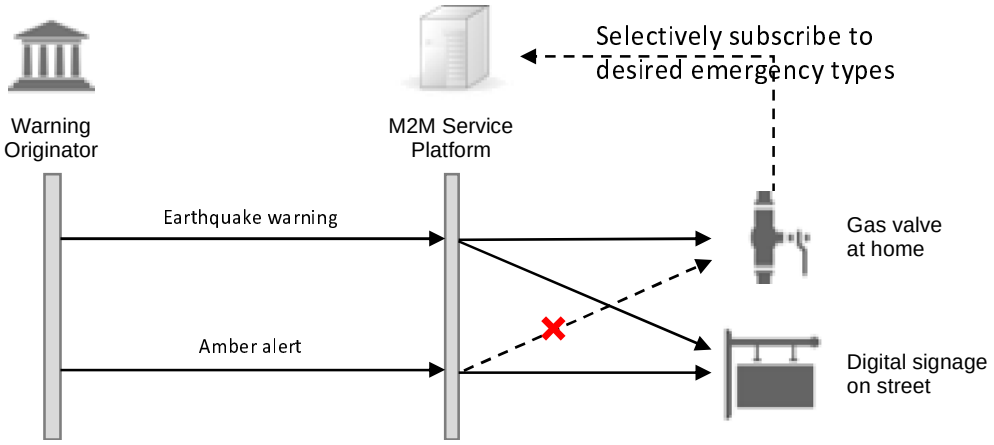


Figure 6.3.9-1: High level illustration of selective respond to type of emergencies

6.3.10 Potential Requirements

This use case scenario can be fulfilled by the existing requirements as defined in oneM2M TS-0002 [i.3], (see Table 6.3.10-1).

Table 6.3.10-1: Related existing requirements as defined in oneM2M TS-0002 [i.3]

Requirement ID	Description	Release
OSR -109 See REQ-2017-0008R02	*The oneM2M System shall enable M2M Gateways to distribute notifications according to how data subscriptions have been grouped/aggregated.*	*Implemented in Rel-3*
OSR-110 See REQ-2017-0008R02	*The oneM2M System shall enable subscriptions to changes to multiple data sources (e.g. oneM2M resources) which aim to generate data publication (i.e. automatic notifications) if and only if the expected changes to each of those multiple resources occur concurrently.*	*Implemented in Rel-3*

The requirements in Table 6.3.10-2 can be considered as additional potential requirements for the use case in oneM2M TS-0002 [i.3].

Table 6.3.10-2: New potential requirement for oneM2M TS-0002 [i.3]

Requirement ID	Description
HLR-xxx	*oneM2M System should support Public Warning Information Model that contains an event type for each emergency situation. (Emergency situation can be earthquake, tsunami, etc.)*

6.4 Release of Emergency Mode

6.4.1 Description

A device perform a predefined emergency task in an emergency mode when a warning message, that is compatible with the Public Warning Information Model, is received. It is necessary to terminate a predefined emergency task and release an emergency mode when an emergency situation ends when following cases happen:

- A warning originator sends a warning message indicating the termination of an emergency situation.
- A timer that a device has and is triggered to start when a warning message is received is expired.
- A user of a device receiving a warning message and performing a pre-defined emergency task manually terminates the emergency mode of a device.

6.4.2 Source

None.

6.4.3 Actors

- Warning originator: Responsible for providing warning notification to citizens in emergency situation.
- M2M Service Platform (MSP): M2M service platform that communicates with UDs and PDs in its M2M system.
- Device: M2M/IoT devices which perform pre-defined emergency tasks in emergency situation.
- User: a person in charge of the management of a device.

6.4.4 Pre-conditions

- A device supports the Public Warning Information Model.
- A device performs emergency tasks in the emergency mode.

6.4.5 Triggers

It is triggered when following cases happen:

- A warning originator sends a warning message indicating the termination of an emergency situation.
- A timer that a device has and is triggered to start when a warning message is received is expired.
- A user of a device receiving a warning message and performing a pre-defined emergency task manually terminates the emergency mode of a device.

6.4.6 Normal Flow

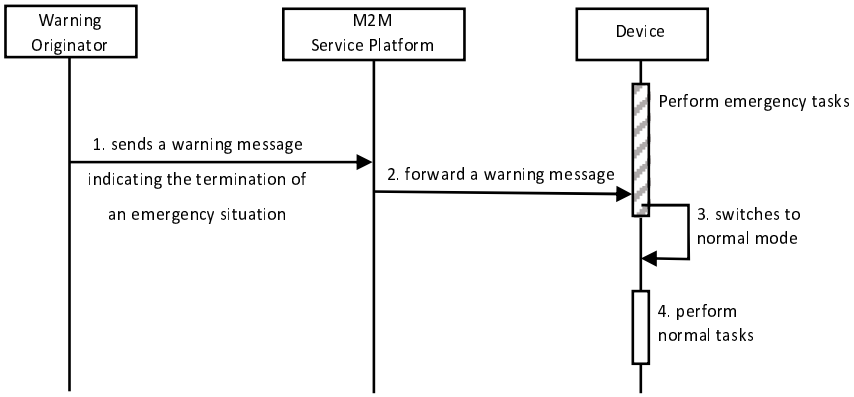


Figure 6.4.6-1: Normal flow for the release of emergency mode

1) A warning originator sends a warning message indicating the termination of an emergency situation.
2) A M2M service platform forwards a warning message indicating the termination of an emergency situation received from a warning originator.
3) A device switches to normal mode when a warning message is received.
4) A device performs normal tasks.

6.4.7 Alternative Flow

A) Triggered by timer

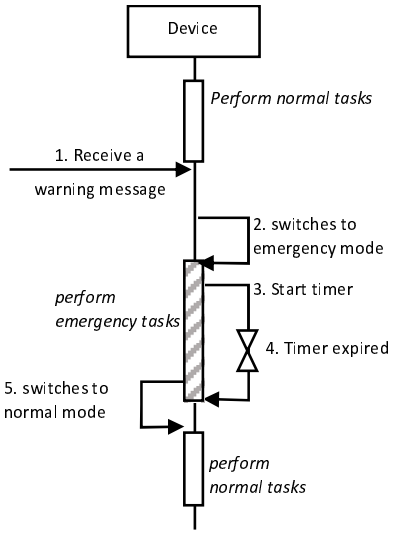


Figure 6.4.7-1: Alternative flow on triggering by a timer

1) A device receives a warning message.
2) The device switches to the emergency mode when a warning message is received and then performs emergency tasks.
3) The device starts a timer to alarm the time to terminate the emergency tasks.
4) The timer is expired.
5) The device switches to the normal mode to perform normal tasks.

B) Triggered by a user

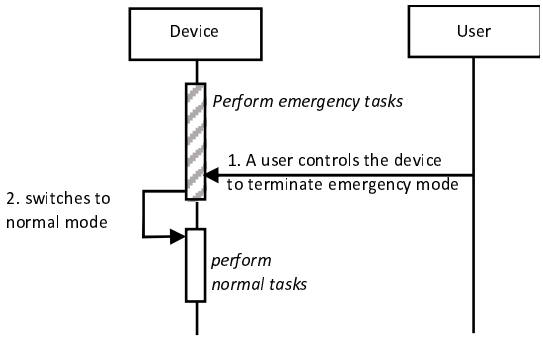


Figure 6.4.7-2: Alternative flow on triggering by a user

1) A user controls the device to terminate the emergency mode.
2) The device switches to the normal mode to perform the normal tasks.

6.4.8 Post-conditions

None.

6.4.9 High Level Illustration

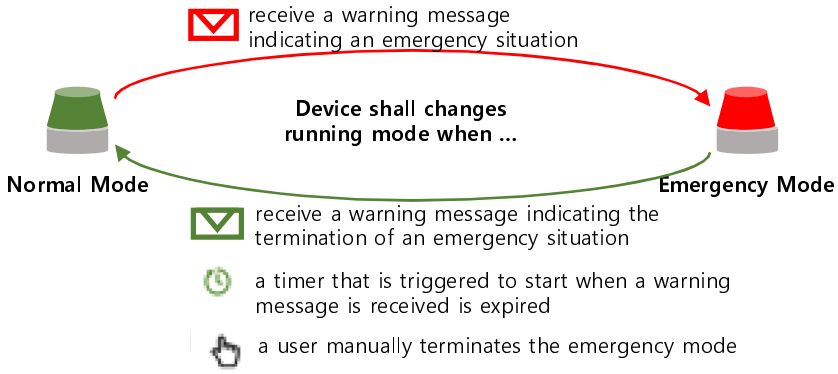


Figure 6.4.9-1: High level illustration of the release of emergency mode

6.4.10 Potential Requirements

The requirements in Table 6.4.10-1 can be considered as additional potential requirements for the use case in oneM2M TS-0002 [i.3].

Table 6.4.10-1: New potential requirement for oneM2M TS-0002 [i.3]

Requirement ID	Description
HLR-xxx	*oneM2M System shall support Public Warning Information Model that contains the emergency mode of a device including timer information.*

6.5 Duplication of Warning Messages

6.5.1 Description

Warning messages used to be periodically distributed by warning originators in order to make sure that warning messages are delivered to devices during an emergency situation. In such case, devices used to receive several warning messages that alert a same emergency situation from a M2M Service Platform so it is necessary to ignore duplicated warning messages if a device already receives a warning message.

6.5.2 Source

None.

6.5.3 Actors

- Warning originator: Responsible for providing warning notification to citizens in emergency situation.
- M2M Service Platform (MSP): M2M service platform that communicates with UDs and PDs in its M2M system.
- Device: M2M/IoT devices which perform pre-defined emergency tasks in emergency situation.

6.5.4 Pre-conditions

- A device is configured to enable the public warning service.
- A device performs its own normal tasks.

6.5.5 Triggers

- A warning originator periodically sends warning messages to alert a same emergency situation until such an emergency situation ends.

6.5.6 Normal Flow

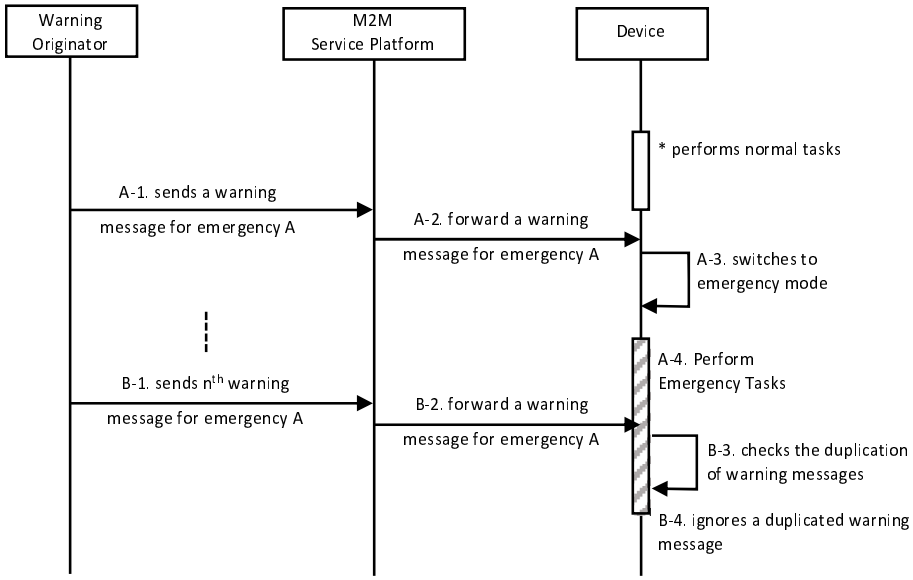


Figure 6.5.6-1: Normal flow for the duplication of warning messages

1) A warning originator sends a warning message for emergency "A".
2) A M2M service platform forwards a warning message for emergency "A" received from a warning originator.
3) A device switches to emergency mode when a warning message is received.
4) A device performs emergency tasks that are pre-defined.
5) The warning originator sends nth warning message for emergency "A".
6) The M2M service platform forwards that warning message for emergency "A".
7) The device checks the duplication of received warning messages.
8) The device ignores a duplicated warning message.

6.5.7 Alternative Flow

None.

6.5.8 Post-conditions

None.

6.5.9 High Level Illustration

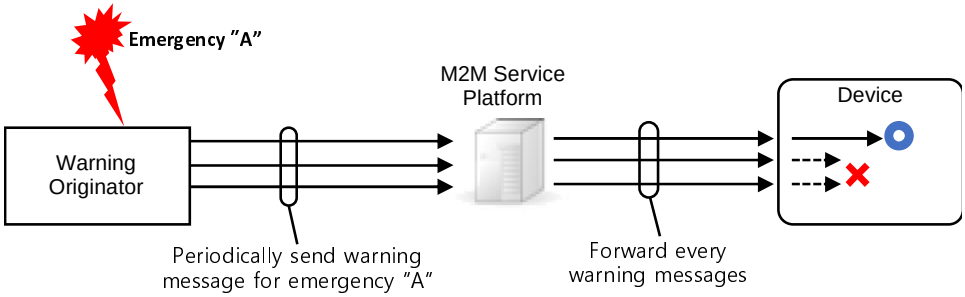


Figure 6.5.9-1: High level illustration of duplication of warning messages

6.5.10 Potential Requirements

This use case scenario can be fulfilled by the existing requirements as defined in oneM2M TS-0002 [i.3], (see Table 6.5.10-1).

Table 6.5.10-1: Related existing requirement as defined in oneM2M TS-0002 [i.3]

Requirement ID	Description	Release
CMR-006 See REQ-2015-0564R02	*The oneM2M System shall support the ability for applications to categorize requested communications (priority, importance, etc.), so that the oneM2M System can adapt its actual communications (scheduling, aggregation, compression, etc.) by taking this categorization into account.*	*Implemented in Rel-1*

The requirements in Table 6.5.10-2 can be considered as additional potential requirements for the use case in oneM2M TS-0002 [i.3].

Table 6.5.10-2: New potential requirement for oneM2M TS-0002 [i.3]

Requirement ID	Description
HLR-xxx	*oneM2M System should support Public Warning Information Model that contains a unique identifier for each emergency situation. (Emergency situation can be earthquake, tsunami, etc.)*

7 Architecture analysis for the new use cases and requirements with current oneM2M system

7.1 Introduction

The use cases of the IoT based public warning services are listed in Table 7.1-1.

Table 7.1-1: Use cases for the IoT Public Warning Service

Use case No.	Title	Description
1	Public warning service triggered by external system	See clause 6.1
2	Enabling and disabling of public warning service	See clause 6.2
3	Opt-in specific type of Public Warning Notification	See clause 6.3
4	Release of Emergency Mode	See clause 6.4
5	Duplication of Warning Messages	See clause 6.5

The following clauses derive possible architectures for oneM2M to support above use cases.

7.2 IoT Public Warning System Architectures

Figure 7.2-1 depicts the high level oneM2M architecture to enable the Public Warning Service. The M2M PWS Gateway is responsible for delivering the warning messages from the Integrated PWS System to M2M Devices through a M2M System. M2M devices can be connected directly to the M2M System via long range communication networks such as LPWA (Low Power Wide Area). Other devices which have only short range communication networks such as ZigBee®, Bluetooth®, etc., can be connected to the M2M System via home or factory gateways. Some of these devices are programmed to initiate performing special functions to react to emergencies upon receiving PWS messages.

In this type of architecture, the M2M PWS Gateway, which is depicted in Figure 7.2-1, acts as an ASN or a MN. A warning message which is generated by the Integrated PWS System contains both human readable and machine readable information. The M2M PWS Gateway extracts machine readable information from CAP messages in XML format to optimize (e.g. reduce message size, change data types) warning messages before deliver the warning message to the M2M System.

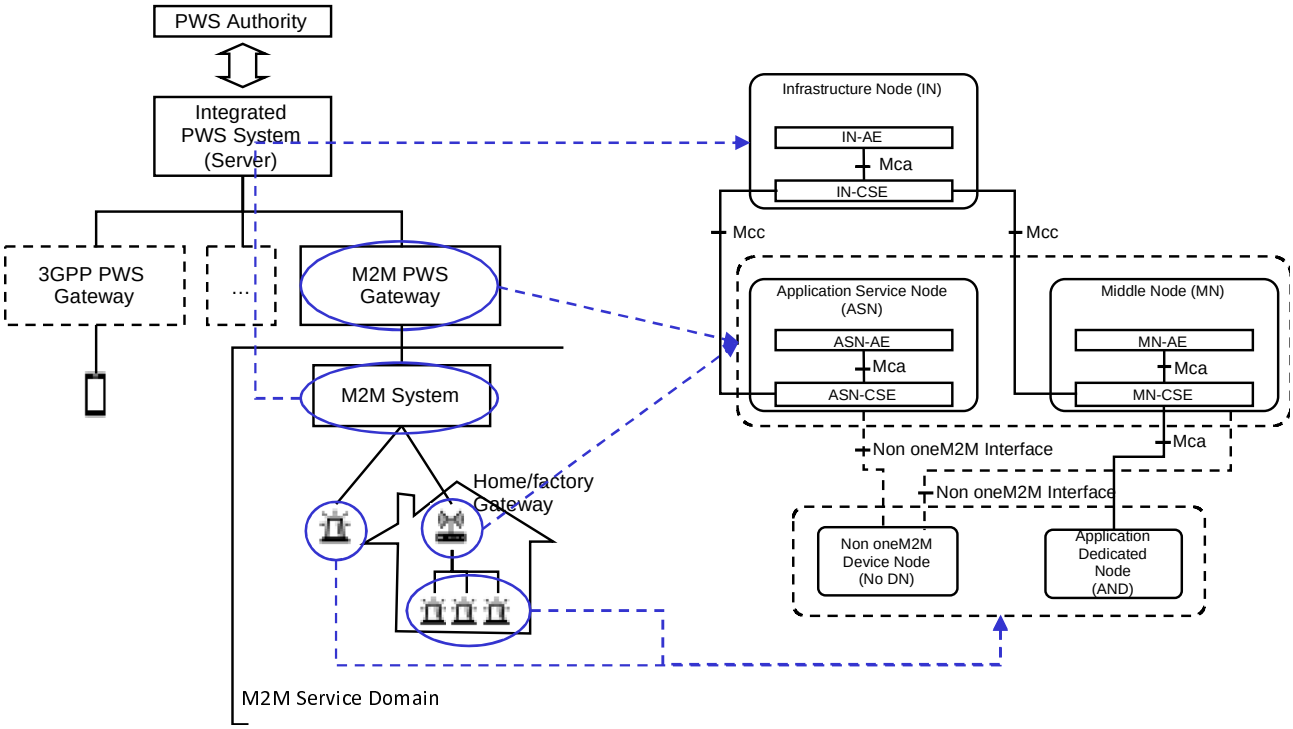


Figure 7.2-1: High Level Architecture for IoT PWS Service

8 Abstract data models for public warning services

8.1 Design principle of information models

8.1.1 Introduction

This clause defines a design principle of the information model for the oneM2M public warning service. Defining an information model is important to ensure interoperability between the devices which are developed individually to provide the same service. In terms of the oneM2M-based public warning service, there are two interfaces which are required to guarantee interoperability by sharing a common information model. The first one is the interface between the oneM2M public warning service gateway and oneM2M system to disseminate the warning message from authority to public devices through the oneM2M system, and the second one is the interface provided by individual devices in the M2M system to trigger emergency tasks when the system received public warning messages.

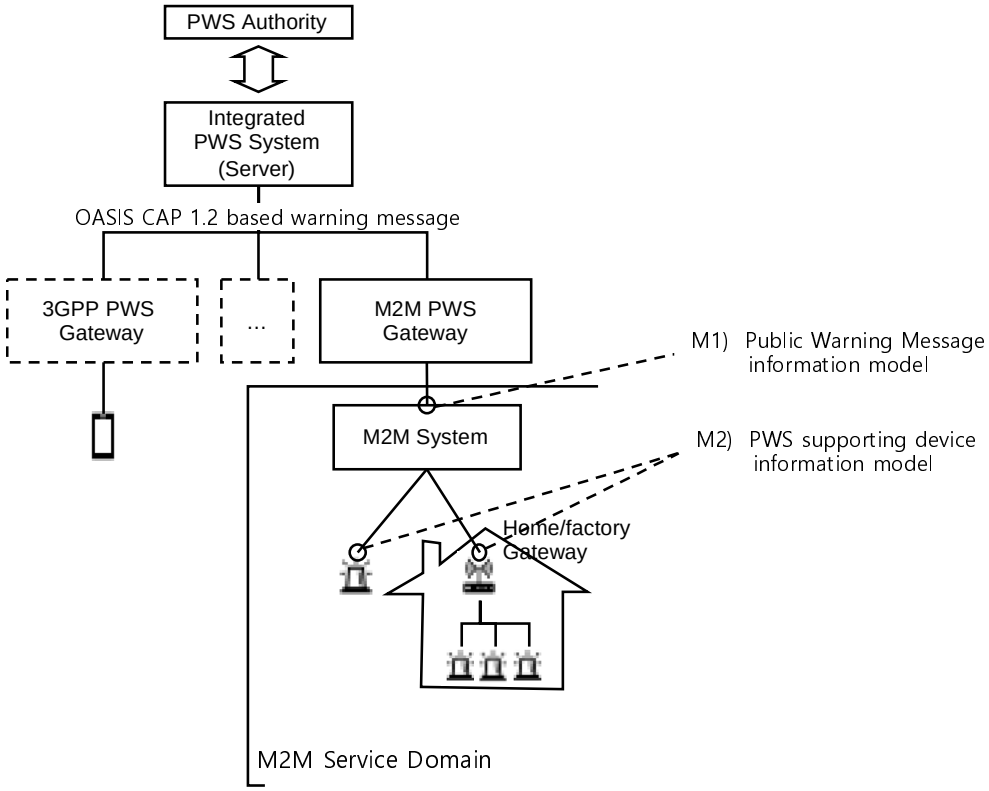


Figure 8.1.1-1: oneM2M based public warning service interfaces

Clause 8.1.2 shows a way to define an information model that can be used to represent emergencies in the oneM2M system based public warning services. By investigating of Common Alerting Protocol (CAP) 1.2 [i.2] message format which is widely used to exchange public warnings between heterogeneous warning systems and applications, information constituting the CAP warning message can be divided into machine interpretable or not. To define oneM2M public warning service information model, machine interpretable information are used as main elements, and other information can be used as optional element. Clause 8.1.3 provides two approaches to define information model for oneM2M devices that supports public warning service features by using the Smart Device Template (SDT) [i.5]. The SDT is a template which is used to model the capabilities, actions and events of smart devices, and used to define information model for home and industrial domain applications in the oneM2M.

8.1.2 Extracting machine interpretable information from CAP public warning message format

8.1.2.1 Information model of OASIS CAP 1.2

The Common Alerting Protocol (CAP) [i.2] is the digital message format designed to exchange all types of emergency alerts and notifications.

Compatibility with the CAP message format is an important factor for integrated operation and functional complementation with existing warning systems. Therefore, compatibility with the CAP message format is important consideration in designing information model of IoT based public warning service.

As a result of the analysis on the structure of the CAP message, the characteristics of each property of the CAP message were provided in terms of name, data type, optionality and machine interpretability as mentioned in clause 8.1.2.2. This information can be used to design an information model of IoT enabled public warning service so that it supports compatibility with CAP based external public warning systems.

A CAP alert message instance is an XML document that consists of an <alert> element as a root element. An <alert> element may contain one or more <info> element, each <info> element may include one or more <area> and/or <resource> element. CAP document object model depicted in Figure 8.1.2.1-1 is designed to minimize operational complexity by eliminating the need for multiple custom interfaces between many warning sources and dissemination systems involved in all-hazard warning.

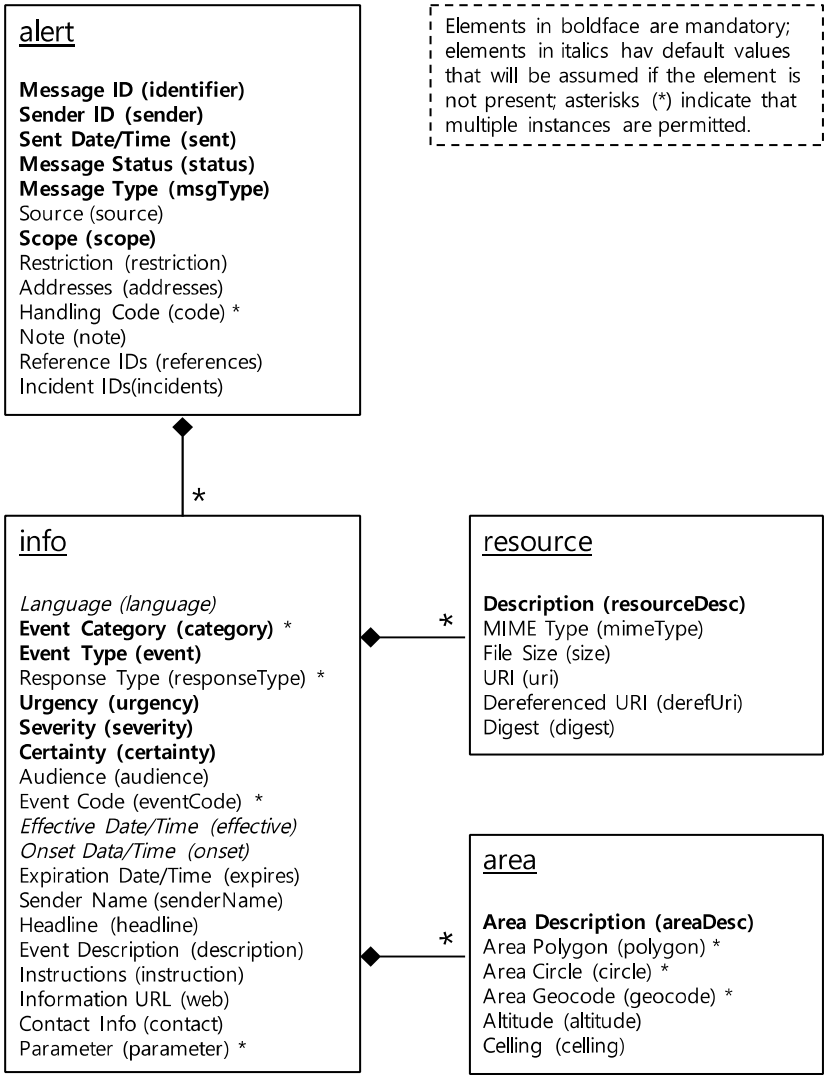


Figure 8.1.2.1-1: CAP document object modelling [i.2]

8.1.2.2 Extracting machine interpretable information from CAP <alert> element

The <alert> element provides basic information for current public warning message that consists of its purpose, source and status, as well as a unique identifier for the current warning message.

Table 8.1.2.2-1: The list of attributes for CAP <alert> element

Name	Type	Optionality	Description	Machine understandability
identifier	xs:string	REQUIRED	The identifier of the alert message, contains a number or string value that uniquely identifying this message.	Interpretable
sender	xs:string	REQUIRED	The identifier of the originator of this alert message. This value should be guaranteed by assigner to be unique globally.	Interpretable
sent	xs:dateTime	REQUIRED	The time and date of the origination of this alert message. This value should be represented in the DateTime format (e.g. "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT)	Interpretable

Name	Type	Optionality	Description	Machine understandability
status	xs:string	REQUIRED	The code to represent the appropriate handling of the alert message receiver. The CAP 1.2 specification [i.2] restricts code values as below: • "Actual" - Actionable by all targeted recipients • "Exercise" - Actionable only by designated exercise participants; exercise identifier should appear in <note> • "System" - For messages that support alert network internal functions • "Test" - Technical testing only, all recipients disregard • "Draft" - A preliminary template or draft, not actionable in its current form	Interpretable
msgType	xs:string	REQUIRED	The code to represent the nature of the alert message. The CAP 1.2 specification [i.2] restricts code values as below: • "Alert" - Initial information requiring attention by targeted recipients • "Update" - Updates and supersedes the earlier message(s) identified in <references> • "Cancel" - Cancels the earlier message(s) identified in <references> • "Ack" - Acknowledges receipt and acceptance of the message(s) identified in <references> • "Error" - Indicates rejection of the message(s) identified in <references>; explanation should appear in <note>	Interpretable
source	xs:string	REQUIRED	Not standardized human readable text identifying an operator or a specific device as the source of the alert message.	Not interpretable
scope	xs:string	REQUIRED	The code to represent the intending scope of distribution for this alert message. The CAP 1.2 specification [i.2] restricts code values as below: • "Public" - For general dissemination to unrestricted audiences • "Restricted" - For dissemination only to users with a known operational requirement (see <restriction>, below) • "Private" - For dissemination only to specified addresses (see <addresses>, below)	Interpretable
restriction	xs:string	CONDITIONAL	Not standardized human readable text to denote the rule for limiting distribution of the restricted alert message. This property appears when "scope" value is "Restricted".	Not interpretable
addresses	xs:string (Separated by white space)	CONDITIONAL	The list of address for a recipients of the alert message. Value of address can be an identifier or an address. This property is required when "scope" value is "Private" and optional when "scope" value is "Public" or "Restricted".	If the value of an address is an identifier, this field would be Machine interpretable
code	xs:string	OPTIONAL	User-defined flag or special code used to handle specially. Multiple code can be presented for an alert message. The format and semantics of the code value are not defined in CAP 1.2 specification [i.2].	Interpretable
note	xs:string	OPTIONAL	Not standardized human readable text clarifying the purpose or significant of the alert message when "status" value is "Exercise" and "msgType" value is "Error".	Not interpretable

Name	Type	Optionality	Description	Machine understandability
references	xs:string (Separated by white space)	OPTIONAL	The list of identifiers for earlier message(s) referenced by this alert message.	Interpretable
incidents	xs:string (Separated by white space)	OPTIONAL	The list of names which are referenced incident(s) of the alert message.	Not interpretable
info	xs:complex Type(<info> element)	OPTIONAL	The container for all component parts of the info sub-element of the alert message. Multiple occurrences are permitted within a single <alert> element to support multiple language or sequence of alert information for an alert message.	n/a (this property is a sub-element described in clause 8.1.2.3)
NOTE: "CONDITIONAL" in the Optionality column can be required or optional according to the value of other properties.				

8.1.2.3 Extracting machine interpretable information from CAP <info> element

The <info> element provides both categorical and textual description of the subject emergency event. It may also provide instructions for appropriate response against the received warning message and extra details (e.g. hazard duration, technical parameters, contact information, links to additional media resource, etc.).

Table 8.1.2.3-1: The list of attributes for CAP <info> element

Name	Type	Optionality	Description	Machine readability
language	xs:language	OPTIONAL	Contains an IETF RFC 3066 [i.7] code value denoting the language of the info sub-element of the alert message.	Interpretable
category	xs:string	REQUIRED	The code denoting the category of the alerting event of the alert message. The CAP 1.2 specification [i.2] restricts code values as below. Multiple category can be presented in an <info> element. • "Geo" - Geophysical (inc. landslide) • "Met" - Meteorological (inc. flood) • "Safety" - General emergency and public safety • "Security" - Law enforcement, military, homeland and local/private security • "Rescue" - Rescue and recovery • "Fire" - Fire suppression and rescue • "Health" - Medical and public health • "Env" - Pollution and other environmental • "Transport" - Public and private transportation • "Infra" - Utility, telecommunication, other non-transport infrastructure • "CBRNE" - Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack • "Other" - Other events	Interpretable
event	xs:string	REQUIRED	Not standardized human readable text describing the type of the subject event of the alert message.	Not Interpretable

Name	Type	Optionality	Description	Machine readability
responseType	xs:string	OPTIONAL	The code denoting the type of recommended response action for the target audience when the alert message received. The CAP 1.2 specification [i.2] restricts code values as below. Multiple responseType can be presented in an <info> element: • "Shelter" - Take shelter in place or per <instruction> • "Evacuate" - Relocate as instructed in the <instruction> • "Prepare" - Make preparations per the <instruction> • "Execute" - Execute a pre-planned activity identified in <instruction> • "Avoid" - Avoid the subject event as per the <instruction> • "Monitor" - Attend to information sources as described in <instruction> • "Assess" - Evaluate the information in this message. (This value should NOT be used in public warning applications.) • "AllClear" - The subject event no longer poses a threat or concern and any follow on action is described in <instruction> • "None" - No action recommended	Interpretable
urgency	xs:string	REQUIRED	The code representing the urgency of the subject event of the alert message. The CAP 1.2 specification [i.2] restricts code values as below: • "Immediate" - Responsive action SHOULD be taken immediately • "Expected" - Responsive action SHOULD be taken soon (within next hour) • "Future" - Responsive action SHOULD be taken in the near future • "Past" - Responsive action is no longer required • "Unknown" - Urgency not known	Interpretable
severity	xs:string	REQUIRED	The code representing the severity of the subject event of the alert message. The CAP 1.2 specification [i.2] restricts code values as below: • "Extreme" - Extraordinary threat to life or property • "Severe" - Significant threat to life or property • "Moderate" - Possible threat to life or property • "Minor" - Minimal to no known threat to life or property • "Unknown" - Severity unknown	Interpretable
certainty	xs:string	REQUIRED	The code representing the certainty of the subject event of the alert message. The CAP 1.2 specification [i.2] restricts code values as below: • "Observed" - Determined to have occurred or to be ongoing • "Likely" - Likely (p > ~50 %) • "Possible" - Possible but not likely (p <= ~50 %) • "Unlikely" - Not expected to occur (p ~ 0) • "Unknown" - Certainty unknown	Interpretable
audience	xs:string	OPTIONAL	Not standardized human readable text describing the intended audience of the alert message	Not understandable

Name	Type	Optionality	Description	Machine readability
eventCode	xs:complexType	OPTIONAL	The definitions of system-specific codes identifying the event type of the alert message. A code definition consists of valueName and value. Multiple eventCode can be presented in an <info> element.	Interpretable
effective	xs:dateTime	OPTIONAL	The effective time of the information of the alert message. This value should be represented in the DateTime format (e.g. "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). If this value is not presented, effective time is assumed to be the same time as in "sent".	Interpretable
onset	xs:dateTime	OPTIONAL	The expected time of the beginning of the subject event of the alert message. This value should be represented in the DateTime format (e.g. "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT).	Interpretable
expires	xs:dateTime	OPTIONAL	The expiry time of the information of the alert message. This value should be represented in the Date Time format (e.g. "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). If this value is not presented, recipient can set own expiration policy.	Interpretable
senderName	xs:string	OPTIONAL	Not standardized human readable name of the agency or authority issuing this alert message.	Not understandable
headline	xs:string	OPTIONAL	Not standardized human readable short headline text of the alert message. 160 characters are recommended.	Not understandable
description	xs:string	OPTIONAL	Not standardized human readable extended description of the hazard or event that occasioned this message.	Not understandable
instruction	xs:string	OPTIONAL	Not standardized human readable instruction describing recommended action to targeted recipients.	Not understandable
web	xs:anyURI	OPTIONAL	The hyperlink URI for an HTML page or text resource to provide additional information for the alert message	Interpretable
contact	xs:string	OPTIONAL	Not standardized human readable text describing the contact for follow-up and confirmation of the alert message.	Not understandable
parameter	xs:complexType	OPTIONAL	The definitions of system-specific parameter associated with the alert message. A parameter definition consists of valueName and value. Multiple parameter can be presented in an <info> element.	Interpretable
resource	xs:complexType(<resource> element)	OPTIONAL	The definitions of all component parts of the resource refers to an additional file. This definition to be used to provide multimedia file to recipients. Multiple resource can be presented in an <info> element.	n/a (This property is a sub-element described in clause 8.1.2.4)
area	xs:complexType(<area> element)	OPTIONAL	The definition of all component parts of the area identifying an affected area. A <info> element may contain one or multiple area definition to identify union of all the included area.	n/a (This property is a sub-element described in clause 8.1.2.5)

8.1.2.4 Extracting machine interpretable information from CAP <resource> element

The <resource> element provides additional information about subject event in the form of a digital asset such as an image or audio resource link.

Table 8.1.2.4-1: The list of attributes for CAP <resource> element

Name	Type	Optionality	Description	Machine readability
resourceDesc	xs:string	REQUIRED	Not standardized human readable description of the type and content of a referenced resource file. EXAMPLE: A map or photograph.	Not understandable
mimeType	xs:string	REQUIRED	The MIME type, as described in IETF RFC 2046 [i.8], identifier describing the referenced resource file.	Interpretable
size	xs:integer	OPTIONAL	The approximate size of the resource file in bytes indicating the size of the referenced resource file.	Interpretable
uri	xs:anyURI	OPTIONAL	The hyperlink URL that can be used to retrieve the resource over the Internet.	Interpretable
derefUri	xs:string	CONDITIONAL	An alternative to the uri resource hyperlink giving the Base64 encoded content of the resource file.	Interpretable
digest	xs:string	OPTIONAL	The SHA-1 hash value of the resource file for validation.	Interpretable
NOTE: "CONDITIONAL" in the Optionality column can be required or optional according to the value of other properties.				

8.1.2.5 Extracting machine interpretable information from CAP <area> element

The <area> element describes a geographic area that specifies the target area to which propagate for the related emergency event.

Table 8.1.2.5-1: The list of attributes for CAP <area> element

Name	Type	Optionality	Description	Machine readability
areaDesc	xs:string	REQUIRED	Not standardized human readable description of the affected area of the alert message.	Not understandable
polygon	xs:string	OPTIONAL	The space-separated list of coordinate pair defines the polygon that identify the affected area of the alert message. Each coordinate value contains geolocation position value as specified in WGS84 standard [i.12]. Multiple polygon in an <area> element is used to identify union of all polygons.	Interpretable
circle	xs:string	OPTIONAL	The space-separated list of coordinates for a centre position and a radius that identify the affected area of the alert message. The first two WGS84 geolocation position value represents the centre position of the circle, and last value represents the radius delineating in kilometres. Multiple circle in an <area> element is used to identify union of all polygons.	Interpretable
geocode	xs:complexType	OPTIONAL	The geographic code identifying the affected area of the alert message. A geocode consists of valueName and value. Multiple geocode can be presented in an <area> element.	Interpretable
altitude	xs:decimal	OPTIONAL	The specific or minimum altitude in feet above mean sea level of the affected area of the alert message.	Interpretable
ceiling	xs:decimal	CONDITIONAL	The maximum altitude in feet above mean sea level of the affected area of the alert message.	Interpretable
NOTE: "CONDITIONAL" in the Optionality column can be required or optional according to the value of other properties.				

8.1.3 Defining information model using SDT

8.1.3.1 Generalize features of public warning service supporting device

As a result of studies on clause 6, generalized features of public warning service supporting device can be draw an use case diagram (Figure 8.1.3.1-1).

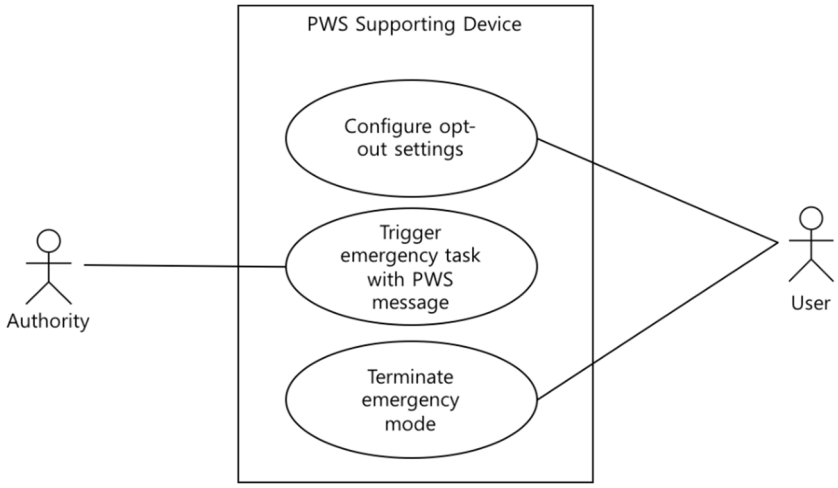


Figure 8.1.3.1-1: Use case for a public warning service supporting device

Figure 8.1.3.1-1 has three use cases:

a) configure opt-out settings;

b) trigger emergency task with PWS message;

c) terminate emergency mode.

In the following clause 8.2.3 and clause 8.2.4 provides an example of definition information model for a device that supporting these use cases.

8.1.3.2 Possible approaches to define information model

Since the public warning service is a cross-domain service, defining a device information model for the public warning service need to be considered any different approaches from the domain specific service domain. The cross-domain service means that a service has been implemented to target two or more application domains (e.g. home, industry, and vehicle domains) rather than to target a single specific application domain. In other points of view, the public warning service is working on a device that provide domain-specific functionalities on peacetime, and provides public warning service on the emergency situation. Therefore, the information model for public warning service should be linked to application-specific information models.

oneM2M TS-0023 [i.4] provides the home appliance information model for home domain devices (e.g. TV, refrigerator, air conditioner, etc.) based on HGI SDT. This clause describes two possible approaches to define an information model for a public warning service on the oneM2M device by showing examples about adding public warning service features to a home appliance information model. The SDT is used to represent the liked relationship between application domain specific information model and public warning service domain information model.

Figure 8.1.3.2-1 depicts an example of defining emergencyWarningDisplay module in the deviceTelevision which is an information model for TV in oneM2M TS-0023 [i.4]. This approach is one of the ways to define features of the public warning service through modification of the original domain-specific information model.

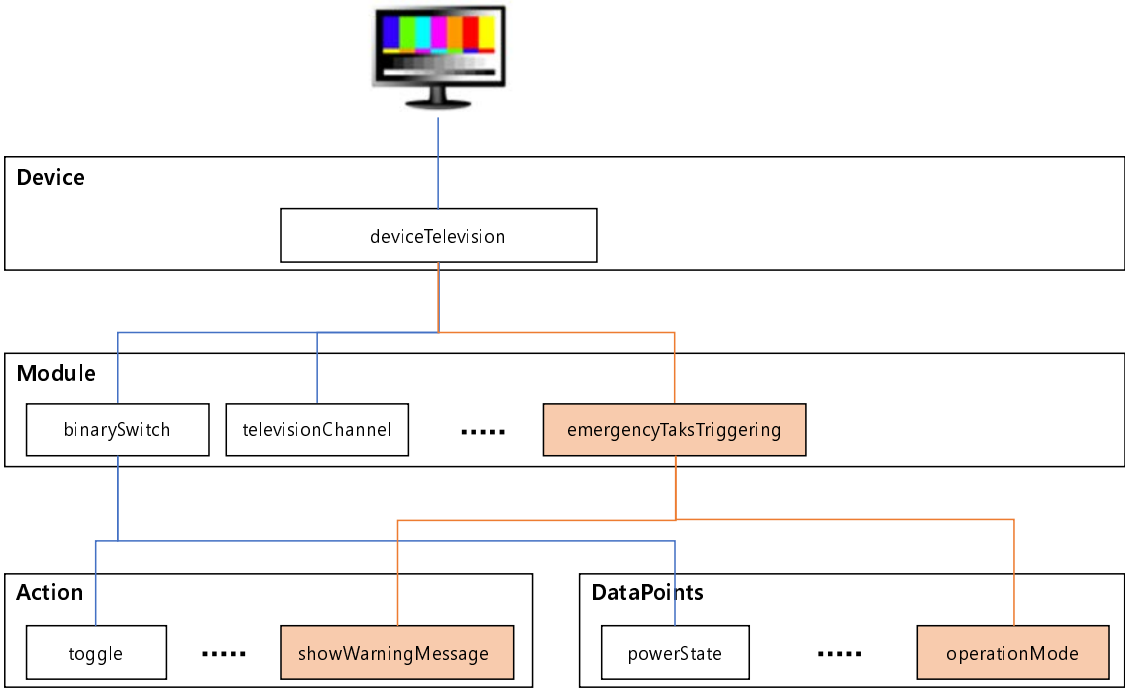


Figure 8.1.3.2-1: An example of the TV information model extension

Figure 8.1.3.2-2 depicts an example of defining a virtual device named devicePWS for public warning service domain. Both the deviceTelevision and the devicePWS are assigned to one physical device TV that supports not only for the home appliance domain but also the public warning service domain in this example. This approach provides the other way to define a virtual device which supports public warning device without modifying the original domain-specific information model.

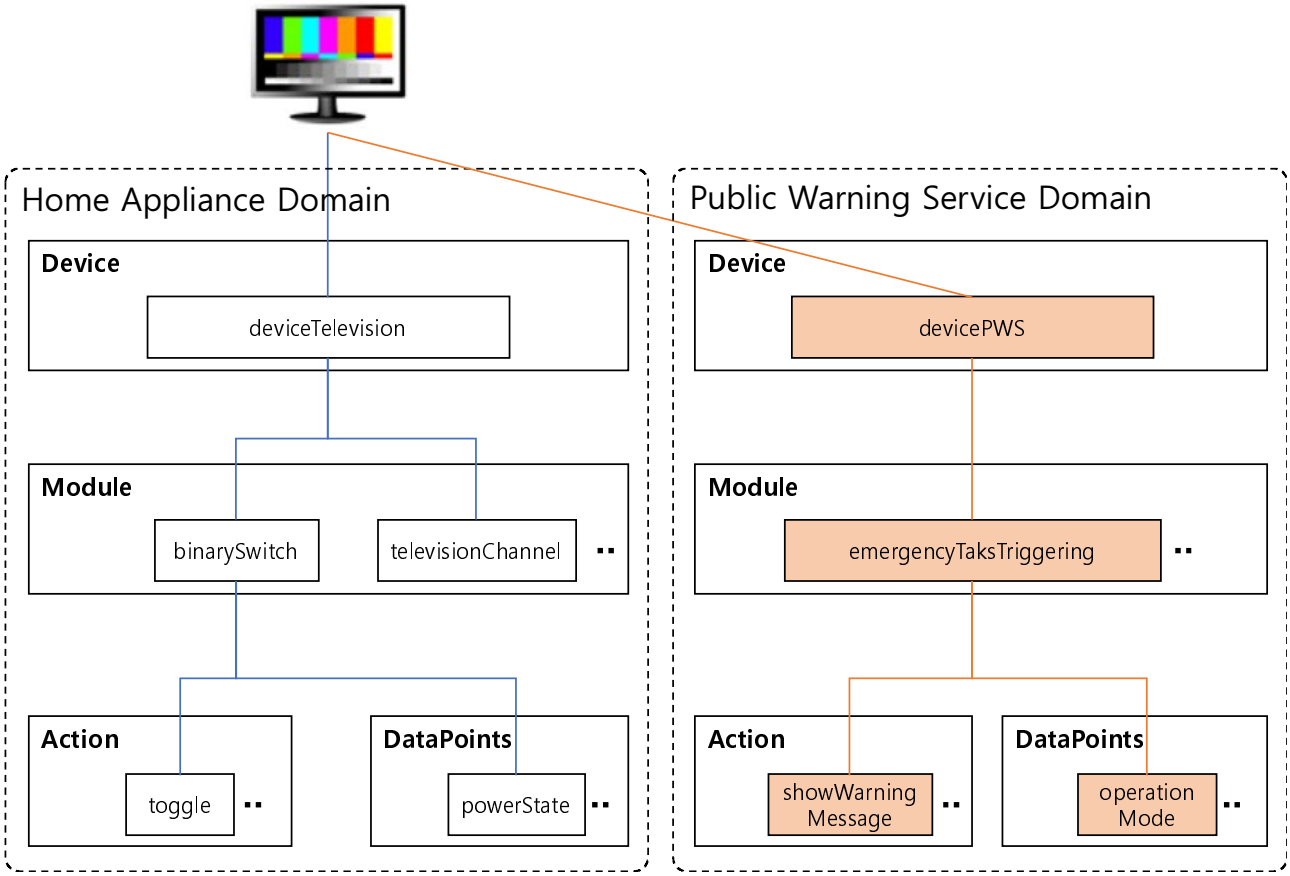


Figure 8.1.3.2-2: An example of a virtual device information model

8.2 Abstract information models

8.2.1 Definition of Data Types

8.2.1.1 Enumeration types

This clause provides enumeration type descriptions for the public warning service domain. To clarify terms for the public warning service domain, the "pws" namespace qualifier will be used in the following clauses.

A. pws:enumAlertStatus

The pws:enumAlertStatus enumeration type represents the appropriate handling of the alert message receiver.

Table 8.2.1.1-1: Interpretation of pws:enumAlertStatus

Value	Name	Interpretation
1	Actual	Actionable by all targeted recipients
2	Exercise	Actionable only by designated exercise participants
3	System	For messages that support alert network internal functions
4	Test	Technical testing only, all recipients disregard
5	Draft	A preliminary template or draft, not actionable in its current form
NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [i.2].		

B. pws:enumMessageType

The pws:enumMessageType represents the nature of the alert message.

Table 8.2.1.1-2: Interpretation of pws:enumMessageType

Value	Name	Interpretation
1	Alert	Initial information requiring attention by targeted recipients
2	Update	Updates and supersedes the earlier message(s)
3	Cancel	Cancels the earlier message(s)
4	Ack	Acknowledges receipt and acceptance of the message(s)
5	Error	Indicates rejection of the message(s)
NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [i.2].		

C. pws:enumAlertScope

The pws:enumAlertScope represents the intending scope of distribution for this alert message.

Table 8.2.1.1-3: Interpretation of pws:enumAlertScope

Value	Name	Interpretation
1	Public	For general dissemination to unrestricted audiences
2	Restricted	For dissemination only to users with a known operational requirement
3	Private	For dissemination only to specified addresses
NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [i.2].		

D. pws:enumEventCategory

The pws:enumEventCategory represents the category of the alerting event of the alert message.

Table 8.2.1.1-4: Interpretation of pws:enumEventCategory

Value	Name	Interpretation
1	Geo	Geophysical (inc. landslide)
2	Met	Meteorological (inc. flood)
3	Safety	General emergency and public safety
4	Security	Law enforcement, military, homeland and local/private security
5	Rescue	Rescue and recovery
6	Fire	Fire suppression and rescue
7	Health	Medical and public health
8	Env	Pollution and other environmental
9	Transport	Public and private transportation
10	Infra	Utility, telecommunication, other non-transport infrastructure
11	CBRNE	Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack
12	Other	Other events
NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [i.2].		

E. pws:enumResponseType

The pws:enumResponseType represents the type of recommended response action for the target audience when the alert message received.

Table 8.2.1.1-5: Interpretation of pws:enumResponseType

Value	Name	Interpretation
1	Shelter	Take shelter in place
2	Evacuate	Relocate to evacuate area
3	Prepare	Make preparations process
4	Execute	Execute a pre-planned activity
5	Avoid	Avoid the subject event
6	Monitor	Attend to information sources
7	Assess	Evaluate the information in this message
8	AllClear	The subject event no longer poses a threat or concern
9	None	No action recommended
NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [i.2].		

F. pws:enumUrgency

The pws:enumUrgency represents the urgency of the subject event of the alert message.

Table 8.2.1.1-6: Interpretation of pws:enumUrgency

Value	Name	Interpretation
1	Immediate	Responsive action should be taken immediately
2	Expected	Responsive action should be taken soon (within next hour)
3	Future	Responsive action should be taken in the near future
4	Past	Responsive action is no longer required
5	Unknown	Urgency not known
NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [i.2].		

G. pws:enumSeverty

The pws:enumSeverty represents the severity of the subject event of the alert message.

Table 8.2.1.1-7: Interpretation of pws:enumSeverty

Value	Name	Interpretation
1	Extreme	Extraordinary threat to life or property
2	Severe	Significant threat to life or property
3	Moderate	Possible threat to life or property
4	Minor	Minimal to no known threat to life or property
5	Unknown	Severity unknown
NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [i.2].		

H. pws:enumCertainty

The pws:enumCertainty represents the certainty of the subject event of the alert message.

Table 8.2.1.1-8: Interpretation of pws:enumCertainty

Value	Name	Interpretation
1	Observed	Determined to have occurred or to be ongoing
2	Likely	Likely (p > ~50 %)
3	Possible	Possible but not likely (p <= ~50 %)
4	Unlikely	Not expected to occur (p ~ 0)
5	Unknown	Certainty unknown
NOTE: Listed names for this enumeration are specified on the CAP 1.2 specification [i.2].		

8.2.1.2 Complex data types

This clause provides complex data types descriptions for the public warning service domain. To clarify terms for the public warning service domain, the "pws" namespace qualifier will be used in the following clauses.

A. pws:TargetArea type

If the originator wants to specify the geographical area which the public warning message will be propagated, the geographical information for the target region may be specified. The Area data type can be used to deliver target geospatial data to which a warning message will be propagated. The geolocation data should be applied to the standard such as GeoJSON [i.13] to improve machine interpretability.

Table 8.2.1.2-1: Structure of pws:TargetArea type

Name	Description	Type	Mandatory/ Optional
polygon	The sequence of coordinate pair to define the polygon that identify the affected area of the alert message. Each coordinate value contains geolocation position value as specified in WGS84 standard [i.12].	GeoJSON	O
circle	The sequence of numeric values to represent a centre position and a radius that identify the affected area of the alert message. The first two values represent geolocation position value WGS84 of the centre position of the circle, and the last value represents the radius delineating in kilometres.	GeoJSON	O
geocode	The geographic code identifying the affected area of the alert message. A geocode consists of valueName and value. Multiple geocode can be presented.	List of <Key, Value> pare	O
altitude	The specific or minimum altitude in feet above mean sea level of the affected area of the alert message.	Number	O
ceiling	The maximum altitude in feet above mean sea level of the affected area of the alert message.	Number	O

B. pws:ExtraResource type

The pws:ExtraResource type is used to pass information about a media resource that contains additional information which includes the event associated with the warning message. For example, if an earthquake warning message generated by an authority includes information about a guide video for an earthquake, the TV may display a warning message and play the guide video by referring to the media resource information included in the pws:ExtraResource.

Table 8.2.1.2-2: Structure of pws:ExtraResource type

Name	Description	Type	Mandatory/ Optional
mimeType	The MIME type, as described in IETF RFC 2046 [i.8], identifier describing the referenced resource file.	String	M
size	The approximate size of the resource file in bytes indicating the size of the referenced resource file.	Number	O
uri	The hyperlink URL that can be used to retrieve the resource over the Internet.	URI	O
derefUri	An alternative to the uri resource hyperlink giving the Base64 encoded content of the resource file.	String	O
digest	The SHA-1 hash value of the resource file for validation.	String	O

C. pws:WarningInfo type

The pws:WarningInfo type contains key information that the authority wants to propagate to the public. This information can be used to recognize and respond to emergencies. Since all data elements contained in WarningInfo need to be machine-readable, the data are passed in the enumeration type defined in clause 8.2.1.1. If necessary, additional information of pws:ExtraResource type and pws:TargetArea which clarify the warning area can be included.

Table 8.2.1.2-3: Structure of pws:WarningInfo type

Name	Description	Type	Mandatory/ Optional
language	Contains an IETF RFC 3066 [i.7] code value denoting the language of the info sub-element of the alert message.	string	O
category	The code denoting the category of the alerting event of the alert message. Multiple category can be presented in an <info> element.	Array of pws:enumEventCategory	M
responseType	The code denoting the type of recommended response action for the target audience when the alert message received. Multiple responseType can be presented.	Array of pws:enumResponseType	O
urgency	The code representing the urgency of the subject event of the alert message.	pws:enumUrgency	M
severity	The code representing the severity of the subject event of the alert message.	pws:enumServerity	M
certainty	The code representing the certainty of the subject event of the alert message.	pws:enumCertainty	M
effective	The effective time of the information of the alert message. If this value is not presented, effective time is assumed to be the same time as in "sent".	DateTime	O
onset	The expected time of the beginning of the subject event of the alert message.	DateTime	O
expires	The expiry time of the information of the alert message. If this value is not presented, recipient can set own expiration policy.	DateTime	O
parameter	The definitions of system-specific parameter associated with the alert message. Multiple parameter can be presented.	List of <Key, Value> pare	O
resource	The definitions of all component parts of the resource refers to an additional file. This definition to be used to provide multimedia file to recipients. Multiple resource can be presented.	Array of pws:ExtraResource type	O
area	The definition of all component parts of the area identifying an affected area. A <info> element may contain one or multiple area definition to identify union of all the included area.	Array of pws:TargetArea type	O

8.2.2 Definition of Message Formats

This clause defines the "Public Warning Message information model" shown in Figure 8.1.1-1. This is a specification of the message that is sent from the authority message to the M2M System to deliver to the device. This message specification can be defined as in Table 8.2.2-1, for the public warning message format for the oneM2M system by extracting machine interpretable attributes among CAP to keep interoperable with CAP 1.2 standard.

Table 8.2.2-1: Structure of public warning message format

Name	Description	Type	Mandatory/ Optional
identifier	The identifier of the alert message, contains a number or string value that uniquely identifying this message.	String	M
sender	The identifier of the originator of this alert message. This value should be guaranteed by assigner to be unique globally.	String	M
sent	The time and date of the origination of this alert message.	DateTime	M
status	The code to represent the appropriate handling of the alert message receiver.	pws:enumAlertStatus	M
msgType	The code to represent the nature of the alert message.	pws:enumMessageType	M
scope	The code to represent the intending scope of distribution for this alert message.	pws:enumScope	M
references	The list of identifiers for earlier message(s) referenced by this alert message.	Array of String	O
info	The container for all component parts of the info sub-element of the alert message. Multiple occurrences are permitted within a single <alert> element to support multiple language or sequence of alert information for an alert message.	Array of pws:WarningInfo type	O

8.2.3 Definition of ModuleClasses

A. configurePWS

Table 8.2.3-1: configurePWS ModuleClass

Doc	ConfigurePWS provides capabilities to change device settings which is related to public warning service including opt-out public warning service.			
Action	**Name**	**Doc**	**Argument**	**Return type**
	OptoutWarningMessage	Setup opt-out status of the device	Name: "command" Type: enum_EMERGENCY_TYPE	enum_EMERGENCY_TYPE
DataPoint	**Name**	**Doc**	**Type**	**Read/Write**
	OptoutState	Current opt-out state of the device: • Off: the device receive all public warning messages. • On: all receive public warning messages will be discarded except opt-out not allowed warning message.	Boolean	Read/Write
Property	**Name**	**Doc**	**Type**	
	N/A			
Event	**Name**	**Doc**	**DataPoint**	
	N/A			

B. emergencyTaskTriggering

Table 8.2.3-2: emergencyTaskTriggering ModuleClass

Doc	EmergencyTaksTriggering provides capabilities to trigger the public warning service enabled devices when a public warning message received.			
Action	**Name**	**Doc**	**Argument**	**Return type**
	ExecuteEmergenceTask	Change operation mode to emergency mode and execute emergency tasks	Name: "PWSMessage" Type: pws:PWSMessage	enum_OPERATION_MODE
DataPoint	**Name**	**Doc**	**Type**	**Read/Write**
	OperationMode	Current operation mode of the device: • Null or 0 --- Normal mode • 1 --- Emergency Mode	enum_OPERATION_MODE	Read/Write
	OptoutState	Current opt-out state of the device.	String	Read only
	ReceivedPWSMessages	List of received public warning messages. This list can be used to check duplicated warning message.	pws:PWSMessage Array	Read only
Property	**Name**	**Doc**	**Type**	
	N/A			
Event	**Name**	**Doc**	**DataPoint**	
	EventTimerExpired	A expiry time specified in a received public warning message has expired	N/A	

C. emergencyModeTermination

Table 8.2.3-3: emergencyModeTermination ModuleClass

Doc	EmergencyModeTermination provides capabilities to stop emergency task which triggered by a public warning message and terminate emergency mode.			
Action	**Name**	**Doc**	**Argument**	**Return type**
	TerminateEmergenceTask	Stop emergency tasks and change operation mode to normal mode	None	None
DataPoint	**Name**	**Doc**	**Type**	**Read/Write**
	OperationMode	Current operation mode of the device: • Null or 0: Normal mode • 1: Emergency Mode	enum_OPERATION_MODE	Read/Write
Property	**Name**	**Doc**	**Type**	
	N/A			
Event	**Name**	**Doc**	**DataPoint**	
	N/A			

8.2.4 Definition of Device

This clause provides the definition of virtual device information for public warning service supporting device using ModuleClasses defined in clause 8.2.3.

Table 8.2.4-1: Modules and properties of devicePWS Device Model

Type	Name	Description	Type	Mandatory/ Optional
Module	configurePWS	See Table 8.2.3-1	-	O
	emergencyTaksTriggering	See Table 8.2.3-2	-	M
	emergencyModeTermination	See Table 8.2.3-3	-	O
Property	initialOptoutStatus	Initial value for opt-out settings	Boolean	O
	Location	Location of PWS device	Location	O

8.3 Resource mapping and manipulation procedures

8.3.1 Introduction

When an external system trigger a public warning message, the oneM2M System should map the warning message to oneM2M resource to make oneM2M devices interpret properly. And next, the oneM2M System disseminate warning message which represented in oneM2M resource to multiple target oneM2M devices at the same time.

Clause 8.3.2 describes how to map public warning messages to oneM2M resources based on public warning service information models that defined in clause 8.2. Clause 8.3.3 shows manipulation procedures to disseminate warning message to multiple target devices in one invocation.

8.3.2 Resource representation of public warning service information model

8.3.2.1 Resource mapping rules

To ensure interoperability between public warning service supporting devices which are provided by multiple venders, abstract information models for public warning service is defined in clause 8.2. The abstract information model for public warning service is defined using SDT 3.0 [i.5] which is used to define home appliance information mode on the oneM2M TS-0023 [i.4]. A SDT based information model can be mapped to oneM2M resource as described in clause 6.2 of the oneM2M TS-0023 [i.4]. This mapping rule can be applied to public warning service information model.

Clauses 8.3.2.2, 8.3.2.3 and 8.3.2.4 show examples of resource mapping for the public warning service information model.

8.3.2.2 Example of device model 'devicePWS'

The present clause shows an example of representation for the device typed 'devicePWS' (see clause 8.2.4 for device model definition of 'devicePWS'). Using the definition, 'devicePWS' model is mapped to [devicePWS] resource which is a specialization of <flexContainer> resource depicted in Figure 8.3.2.2-1.

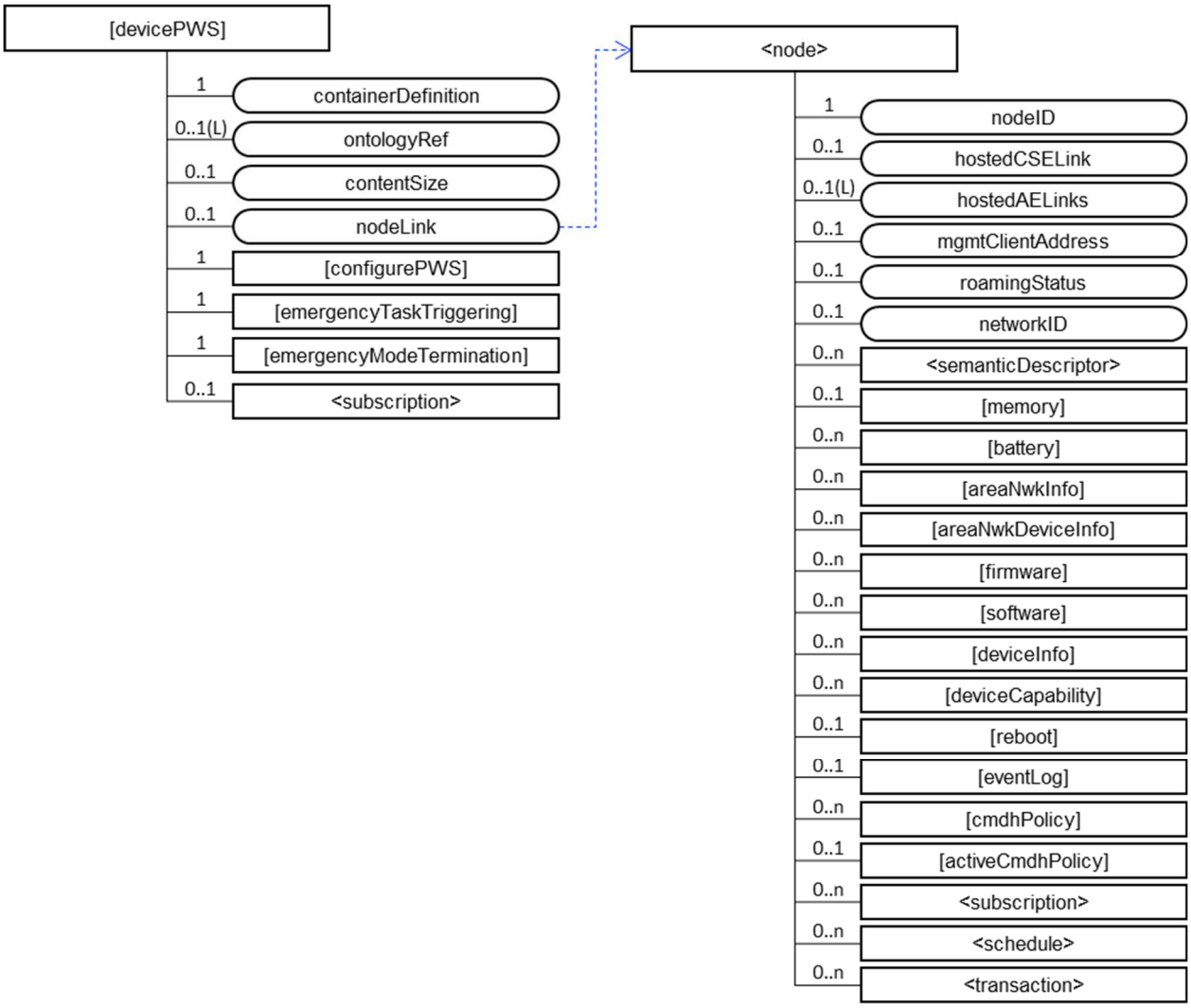


Figure 8.3.2.2-1: Structure of *[devicePWS]* resource

The [devicePWS] resource contains the child resource specified in Table 8.3.2.2-1. Three module classes of the 'devicePWS' device model is mapped as child resource type of the [devicePWS] resource.

Table 8.3.2.2-1: Child resources of *[devicePWS]* resource

Child Resources of *[devicePWS]*	Child Resource Type	Multiplicity	Description
[variable]	*<flexContainer> as defined in the specialization [configurePWS]*	0..1	This resource is used to map 'configurePWS' ModuleClass defined in clause 8.2.3.
[variable]	*<flexContainer> as defined in the specialization [emergencyTaskTriggering]*	0..1	This resource is used to map 'emergencyTaskTriggering' ModuleClass defined in clause 8.2.3.
[variable]	*<flexContainer> as defined in the specialization [emergencyModeTermination]*	0..1	This resource is used to map 'emergencyModeTermination' ModuleClass defined in clause 8.2.3.
[variable]	*<subscription>*	0..n	See clause 9.6.8 in oneM2M TS-0001 [i.9].

The [devicePWS] resource contains the attributes specified in Table 8.3.2.2-2.

Table 8.3.2.2-2: Attributes of *[devicePWS]* resource

Attributes of *[deviceAirConditioner]*	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
resourceID	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
resourceName	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
parentID	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
expirationTime	1	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
creationTime	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
lastModifiedTime	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
labels	0..1	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
dynamicAuthorizationConsultationIDs	0..1 (L)	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
stateTag	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
creator	0..1	RW	See clause 9.6.35 in oneM2M TS-0001 [i.9].
containerDefinition	1	WO	The value is "org.onem2m.pws.device.pwsdevice".
ontologyRef	0..1	RW	See clause 9.6.35 in oneM2M TS-0001 [i.9].
contentSize	1	RO	See clause 9.6.35 in oneM2M TS-0001 [i.9].
nodeLink	1	RO	nodeLink attribute links to a <node> resource that is hosted on the same hosting CSE of the <flexContainer>. See clauses 6.2.2 and 6.2.3 in oneM2M TS-0023 [i.4] for more details.

8.3.2.3 Example of ModuleClass 'emergencyTaskTriggering'

The [*emergencyTaskTriggering*] resource is used to trigger emergency task of public warning supporting device. The [*emergencyTaskTriggering*] resource is a specialization of the <*flexContainer*> resource.

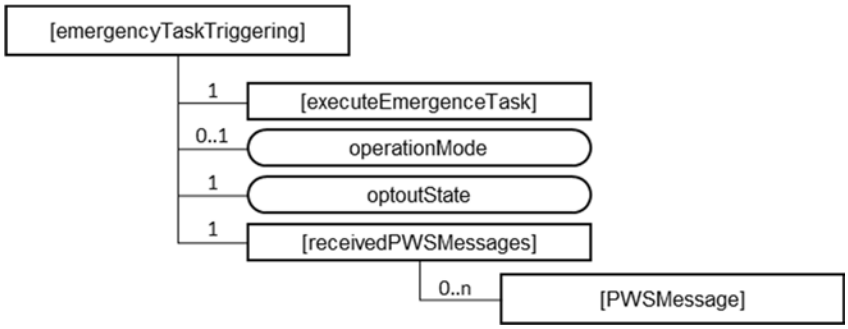


Figure 8.3.2.3-1: Structure of *[emergencyTaskTriggering]* resource

The *[emergencyTaskTriggering]* resource contains the child resource specified in Table 8.3.2.3-1. The 'executeEmergenceTask' action mapped to the [executeEmergenceTask] resource as a specialization of <flexContainer> and 'receivedPWSMessages' data point is mapped to the [receivedPWSMessage] resource. [receivedPWSMessage] also a specialization of <flexContainer>.

Table 8.3.2.3-1: Child resources of *[emergencyTaskTriggering]* resource

Child Resources of *[emergencyTaskTriggering]*	Child Resource Type	Multiplicity	Description
[variable]	*<flexContainer> as defined in the specialization [*executeEmergenceTask*]*	1	This resource is used to map 'executeEmergenceTask' Action defined in clause 8.2.3.
[variable]	*<flexContainer> as defined in the specialization [receivedPWSMessages]*	1	This resource is used to map 'receivedPWSMessages' DataPoint defined in clause 8.2.3. The [receivedPWSMessages] resource contains list of [PWSMessage] specialization of <flexContainer> to store received warning messages.
[variable]	*<subscription>*	0..n	See clause 9.6.8 in oneM2M TS-0001 [i.9].

The *[emergencyTaskTriggering]* resource contains the attributes specified in Table 8.3.2.3-2. The 'operationMode' and 'optoutState' data point mapped to attributes of [emergencyTaskTriggering] resource.

Table 8.3.2.3-2: Attributes of *[emergencyTaskTriggering]* resource

Attributes of *[binarySwitch]*	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
resourceID	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
resourceName	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
parentID	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
expirationTime	1	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
creationTime	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
lastModifiedTime	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
labels	0..1	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
dynamicAuthorizationConsultationIDs	0..1 (L)	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
stateTag	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
creator	0..1	RW	See clause 9.6.35 in oneM2M TS-0001 [i.9].
containerDefinition	1	WO	The value is "org.onem2m.pws.moduleclass.emergencyTaskTriggering".
ontologyRef	0..1	RW	See clause 9.6.35 in oneM2M TS-0001 [i.9].
contentSize	1	RO	See clause 9.6.35 in oneM2M TS-0001 [i.9].
operationMode	1	RW	See clause 8.2.3.
optoutState	1	RW	See clause 8.2.3.

8.3.2.4 Example of Action 'executeEmergenceTask'

The [*executeEmergenceTask*] resource is used to share information regarding the modelled execute emergence task as an Action. The [*executeEmergenceTask*] resource is a specialization of the <*flexContainer*> resource.

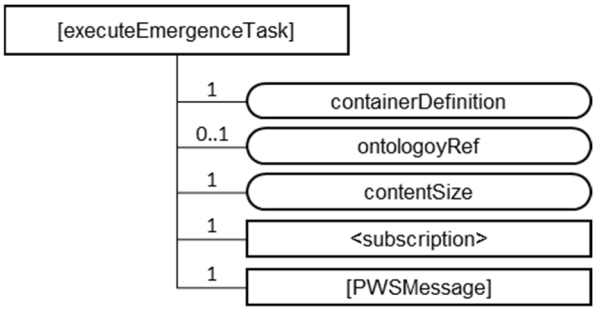


Figure 8.3.2.4-1: Structure of *[executeEmergenceTask]* resource

The *[executeEmergenceTask]* resource contains the child resource specified in Table 8.3.2.4-1.

Table 8.3.2.4-1: Child resources of *[executeEmergenceTask]* resource

Child Resources of *[toggle]*	Child Resource Type	Multiplicity	Description
[variable]	*<flexContainer> as defined in the specialization [PWSMessage]*	1	This resource is used to map the 'PWSMessage' parameter of 'executeEmergenceTask' Action defined in clause 8.2.3.
[variable]	*<subscription>*	0..n	See clause 9.6.8 in oneM2M TS-0001 [i.9].

The *[executeEmergenceTask]* resource contains the attributes specified in Table 8.3.2.4-2.

Table 8.3.2.4-2: Attributes of *[executeEmergenceTask]* resource

Attributes of *[toggle]*	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
resourceID	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
resourceName	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
parentID	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
expirationTime	1	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
accessControlPolicyIDs	0..1 (L)	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
creationTime	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
lastModifiedTime	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
labels	0..1	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
dynamicAuthorizationConsultationIDs	0..1 (L)	RW	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
stateTag	1	RO	See clause 9.6.1.3 in oneM2M TS-0001 [i.9].
creator	0..1	RW	See clause 9.6.35 in oneM2M TS-0001 [i.9].
containerDefinition	1	WO	The value is "org.onem2m.pws.moduleclass.emergencyTaskTriggering.executeEmergenceTask".
ontologyRef	0..1	RW	See clause 9.6.35 in oneM2M TS-0001 [i.9].
contentSize	1	RO	See clause 9.6.35 in oneM2M TS-0001 [i.9].
nodeLink	0..1	RW	Not applicable to an Action specialization. This attribute is not present in an instantiation of this resource.

8.3.3 Manipulation procedures with group APIs

8.3.3.1 Warning message delivery using group fan-out

The oneM2M group APIs are useful to deliver warning messages to multiple devices at the same time. Group APIs enable the oneM2M System to perform bulk operations on multiple resources that are member of a group. In addition, group APIs support bulk operations to multiple resources of interest and aggregates the results.

Figure 8.3.3.1-1 illustrates overall procedure to deliver warning message to multiple member devices of a <group> resource by creating a warning message to the target <group> resource or the <fanOutPoint> virtual child resource of the target <group> resource.

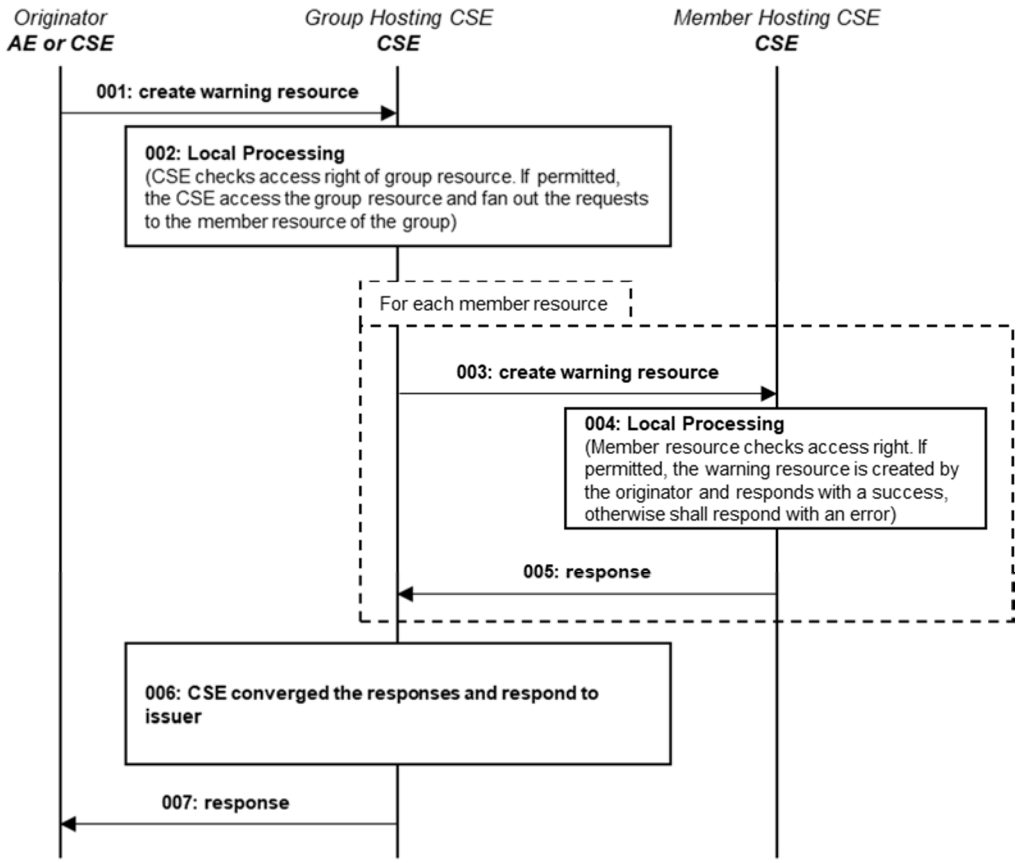


Figure 8.3.3.1-1: Disseminate warning message using <group> resource

001: The Originator should request to create the resource that representing the warning message for same emergency event in all member resources belonging to an existing <*group*> resource by using a CREATE operation. The Request may address the virtual child resource <*fanOutPoint*> of the specific <*group*> resource of a group Hosting CSE. The Originator may be an AE or CSE.

002: The Group Hosting CSE should check if the Originator has CREATE privilege in the <*accessControlPolicy*> resource referenced by the *membersAccessControlPolicyIDs* in the <*group*> resource. If permitted, generate fan out requests addressing to the member hosting CSE.

003: For each member of <group> resource, The Group Hosting CSE requests to create warning message representing resource using generated fan out request.

004: The Member Hosting CSE should check if the original Originator has the CREATE permission on the addressed resource. Upon successful validation, perform the create procedures for the warning message representing resource type of addressed.

005: Send the corresponding response to the Group Hosting CSE.

006: After receiving the responses from the members hosting CSEs, respond to the Originator with the aggregated results and the associated members list.

007: The Group Hosting CSE send converged responses from members hosting CSEs to the Originator.

8.3.3.2 Warning message delivery using sub-group fan-out

To organize members of a group, a <group> resource contains list of member resource IDs in the memberID attribute. Each member ID should refer to a member resource or a sub-group resource of the <group>. The oneM2M system supports hierarchical group by using sub-group features.

Figure 8.3.3.2-1 depicts an example of a hierarchical group organization to support delivering warning messages to target area selectively.

Hierarchical group can be applied to all multi-level categorizable concepts(e.g. type of devices, type of emergency events and severity of warning etc.).

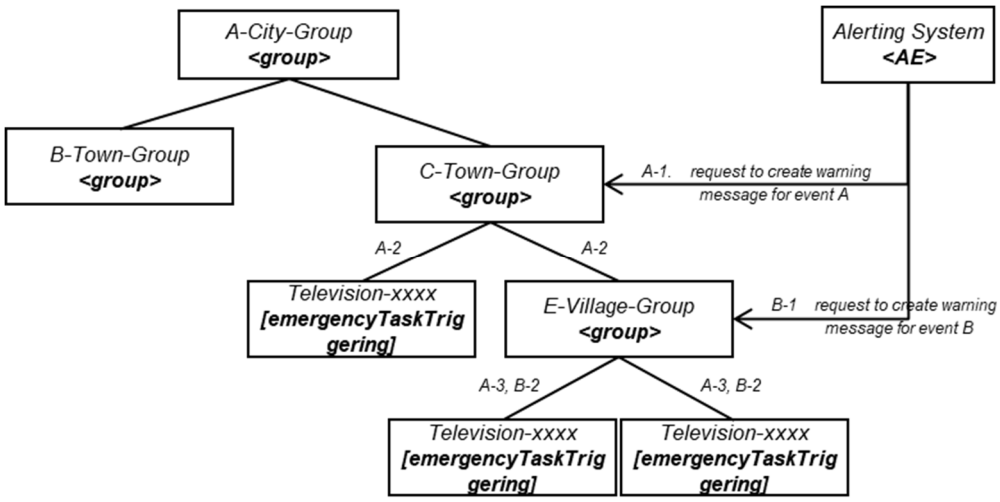


Figure 8.3.3.2-1: Example of <group> resource organization for disseminate warning messages

(A-1) request to create a warning message instance to a target <group> resource (e.g. C-Town-Group) to disseminate warning for emergence event (Warning-A)

(A-2) fan out the requested operation to all members of the group. A member can be a <flexContainer> specialization of [emergencyTaskTriggering] (See clause 8.2.3) or a sub-group

(A-3) fan out the requested operation repeatedly if fanned out target is a sub-group

(A-2, A-3) eventually, All members including members in sub-group can receive the request to create warning message instance for emergency event A

(B-1) request to create a warning message instance to a target <group> resource (e.g. C-Town-Group) to disseminate warning for emergence event (Warning-B)

(B-2) fan out the requested operation to all members of the group. eventually, All member devices of the target <group> resource (e.g. C-Town-Group) receive the request to create warning message instance for emergency event B

9 Conclusion

When IoT devices or applications become aware of a emergencies, devices and applications respond automatically to minimize risks in time of emergency. Some of devices and applications can recognize an emergency situation from their own context information, but other devices and applications which have no context aware functionalities need to be triggered by external systems with sufficient and machine interpretable emergency information to respond to emergencies.

The present document provides results of studies on how to represent public warning information on the oneM2M system and how to deliver warning messages to oneM2M devices efficiently. For the reasons of interworking with external system and efficiency, a HGI SDT 3.0 [i.3] based design principle for public warning service is introduced (clause 8.2). And by showing some examples to propagate warning messages using oneM2M group fan-out feature, the present document proposes a guide for implementing public warning service using oneM2M system (clause 8.3).

The present document will lead to a normative work that will contain more detail information models to support interwork within external systems, oneM2M devices and any other applications for public warning service implementation.

History

Document history		
V4.0.0	April 2022	Publication