CEN/WS CER

Date: 20XX -XX

prCWA CER:2023

Secretariat: ASRO

Collaborative emergency response – Common addressing format and emergency identification protocol

ICS:

CCMC will prepare and attach the official title page.

Contents

European foreword

This CEN Workshop Agreement (CWA xxxxx:2023) has been developed in accordance with CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid prototyping to standardization" and with the relevant provision of European Committee for Standardization (CEN)/European Committee for Electrotechnical Standardization (CENELEC) Internal Regulations – Part 2. It was approved by a Workshop of representatives of interested parties on 2022-02-18, the constitution of which was supported by CEN following the public call for participation made on 2021-12-17. However, this CEN Workshop Agreement does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

This CEN Workshop Agreement (CWA) is based on the results of the EU-funded research project STRATEGY, which received funding from the European Union's HORIZON 2020 research and innovation programme under grant agreement (GA) N° 883520.

The final text of this CEN Workshop Agreement was submitted to CEN for publication on xxxxxxxxxx.

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. CEN-CENELEC policy on patent rights is described in CEN-CENELEC Guide 8 "Guidelines for Implementation of the Common IPR Policy on Patent". CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk.

The following organizations and individuals developed and approved this CEN Workshop Agreement.

- Chairperson: Mr. Leonidas Perlepes, Greece;
- Secretariat: Mrs. Diana Iorga, ASRO (Romanian Standards Association);
- Satways Ltd. (Ilias Gkotsis, Giannis Chasiotis, Dimitris Diagourtas, Antonis Kostaridis, George Eftychidis, Alexios Pagkozidis, Aikaterini Poustourli, Katerina Valouma), Greece;
- Special Telecommunication Service (Ionel-Sorinel Vasilca, Madalin-Virgil Mihai, Andrei-Razvan Mihalache, Simion Tatucu, Daniel-Ionut Rata, Daniela Viorela Derscariu, Georgiana-Cristina Sabareanu, Andreea-Stefania Gradisteanu, Florin Feticu, Marin Dascalu), Romania;
- Unida de Militar Laboratorial de Defesa Biológica e Química/Centro de Investigação da 27 Academia Militar (U28MLDBQ/CINAMIL) (Wilson Antunes, Luís Carvalho), Portugal;
- Institute of Communication and Computer Systems, ICCS (Spyridon Athanasiadis, Eleftherios Ouzounoglou), Greece;
- CBRNE Ltd (Kelly Dominic), UK;
- Corpo Nazionale del Vigili del Fuoco (Paolo Muneretto), Italy;
- Ministry of the Interior - Digital Civil Protection (Olivier Regnault, Jean-Paul Preaux, Nader Mortada), France;
- Public Safety Communication Europe (PSCE) (David Lund, Marie-Christine Bonnamour, Anthony Lamaudiere), Belgium;
- Proactima AS (Ivar Konrad Lunde), Norway;

- UIC (International Union of Railways) (Laura Petersen), France;
- INLECOM (Loredana Mancini), Ireland;
- Health Security Agency (Louise Davidson), UK;
- ENTENTE (EPLFM) ECASC (Philippe Meresse), France;
- Ministries of Transport, Territories and Sea (Romain Cazzato), French;
- Deep Blue SRL (Alessia Golfetti, Andrea Capaccioli), Italy;
- Joint Research Centre (Monica Cardarilli), Italy;
- EUCENTRE Foundation (Chiara Casarotti), Italy;
- Kentro Meleton Asfaleias KEMEA (Georgios Sakkas, Ioannis Tsaloukidis), Greece;
- INOV INESC Inovacao (Gabriel Pestana, Tiago Rocha da Silva), Portugal;
- Hellenic Rescue Team (Iosif Vourvachis, Lorenzo Nerantzis), Greece;
- ATOS (Dario Ruiz Lopez), Spain;
- ETRA (Eduardo Villamor Medina, Eva María Muñoz Navarro), Spain;
- RISE Research Institutes of Sweden (Francine Amon), Sweden;
- Hellenic Fire Service (Georgios Karditsas), Greece.

Introduction

Nowadays, the collaboration and sharing of information among public and private safety agencies during an emergency are critical. Cross-border, large-scale and extensive emergencies require the involvement of public safety agencies, which in the case of the EU Civil Protection Mechanism activation can come from different countries. The usage of electronic solutions (e.g. Incident management systems) by these agencies in order to enable the collaboration and sharing of operational information is required. However, the lack of a common inventory that could host and share, each agency's information sharing capabilities, policy and technical details, infects the efficiency of the agencies' collaboration.

This workshop proposes a common mechanism that will host the communication details of the agencies around the EU, centrally. This mechanism will enable the automatic indexing and discovery of these agencies, covering all the policies and technical details that should be known among agencies, in order to initiate any sharing of operational information. A key feature of this mechanism is a common identification protocol that should be adopted by the agencies, in order to be uniquely identified.

This CEN Workshop Agreement (CWA) has been elaborated as part of the EU-funded research project STRATEGY (https://strategy-project.eu/), which received funding from the European Union's HORIZON 2020 research and innovation programme under grant agreement (GA) N° 883520. More specifically, upon investigation of the standardisation universe across its thematic streams of research and prioritisation of the identified gaps against the operational perspective of end-users, STRATEGY underlined the need and supported the drafting of this CWA.

1 Scope

This CWA specifies a hierarchical naming system for public and private safety agencies and emergency authorities. It covers a common addressing format to be used by authorities, in order to uniquely be identified. This addressing format identifies the agencies and their teams/departments, enabling the quick and easy selection of the agencies that should share a specific piece of information.

Additionally, the specifications of an emergency discovery mechanism are provided, enabling the hosting, indexing and discovery of the available agencies, through the usage of their unique address. Each agency will be represented by a record on the mechanism that will associate the operational and technical characteristics of the agency with the related unique address. Specifications on the data structures and the functionalities that are required to register and get details about an agency are provided.

The message can be targeted to the designated groups such as the incident management and command & control system designers and engineers and decision-makers in emergency management.

2 Normative references

The following documents are referred to in the text in such a way that either a part or all of their content constitutes the requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN ISO 22300:2021, *Societal security — Terminology*

3 Terms and definitions

For the purpose of this document, the terms and definitions given in EN ISO 22300 apply, together with the following.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
communication node
a facility owned by an agency, which may provide operational information messages to other nodes from the same or other agencies in order to share with them part of the event information held at the node. The facilities which can create messages include, but are not limited to, fixed control rooms, mobile control rooms, and coordination rooms set up for a specific event.

4 Emergency Identification Protocol

Effective crisis management requires efficient communication and access to critical information before, during and after operations to ensure public safety and security in disasters. Inter-connectedness and cooperation between different public safety agencies and rescue teams is essential for saving lives and protecting assets. When it comes to organising an effective crisis management response, it is not the number of different disaster definitions that may have an impact on the field work but rather the lack of common way for communication. [1]

The Renewed EU Internal Security Strategy in Action (2018) clearly states the need for improved and more coordinated cooperation within its borders between national civil protection services in disaster response and crisis management and has set as cross-cutting priorities: the Information exchange and interoperability; the availability of data and strengthened links between external and internal dimensions of security. [2]

Thus, the information sharing in the three horizontal layers (field operations layer, command and control layer and administrative layer) identified in crisis management is required. In more detail, the direct communication between acting response units is required within the field operations layer, the command and control layer covers the sharing of information on all assets, personnel and units while the administrative layer requires the sharing of external capacities that can be provided and the strategic decisions on appeals for assistance that may occur.

A network of operational collaboration among the public safety agencies and authorities around the Europe could support these communication requirements.

Usually, public safety agencies have more than one communication node (e.g. multiple command centres, response planning teams etc.) that would require communication with the related communication nodes of other agencies before, during and after a crisis. The number of communication nodes that will be used per agency is highly dependent on each agency's responsibilities, its internal hierarchical structure and the type of communication/collaboration each agency should have with the other agencies.

All these parameters, introduce additional complexity to the creation of a common network of operational collaboration among public safety agencies and organisations.

The first requirement of this operational network of public safety agencies is the unique identification of each of the communication nodes that will be connected to it. The common emergency identification protocol (EIP), that is proposed, describes a common addressing format to be be adopted by all agencies, in order for related communication nodes to be uniquely identified. The format used for the nodes' identification has been designed to represent the operational capabilities and characteristics of each node while being in a language understandable either by the persons or the applications.

The identity format that is proposed, is composed of a number of properties (that each node has) concatenated into multiple layers using the dot (.) special character. Thus, the hierarchical structure of the organisations/agencies is supported. An example of this identity is following:

Country.AgencyType.Agency

The first three properties that are used in the identity should be the following:

- **Country:** The first property should mention the country of the organization that the node belongs to. Each country should be represented by its acronym as specified in ISO 3166-3:2020. The list of formerly used names of countries and their code elements is available online at the ISO Online Browsing Platform at https://www.iso.org/obp/ui/#search/code/. E.g. gr for Greece, fr for France, it for Italy etc.

- **AgencyType:** The second property should mention the type of organization that the node belongs to. A nonexhaustive list of the predefined agency types is:
    - fire
    - law_enforcement
    - emergency_health_case
    - civil_protection
    - coast_guard
    - border_security

  - search_&_rescue
  - 112
  - military
  - regional_authority
  - municipal_authority
  - critical_infrastructure
  - volunteers
  - international_agencies (e.g. EU,UN, …)
  - water_supply
  - electricity_supply
  - motorway
- **Agency:** The third property should mention the name of the organization/agency that the node belongs to. E.g. police, carabinieri, etc.

Except for the three elements that should be placed at the start of the nodes' identifier, any node is free to add additional properties, in order to further detail and describe its capabilities and responsibilities. For example, a property for the scope of the agency (e.g. planning, response etc.) or the agency department's internal identifier (e.g. police111, fire231, etc.) could be used.

The following Table 1 contains a list of examples of the possible usage of this emergency identification protocol.

Table 1 — Emergency Identification Protocol

AGENCY	EIP
Italian Carabinieri Agency	it.law_enforcement.carabinieri
Greek Fire Service Agency	gr.fire.fire_service
Greek Fire Service Agency, Command & Control Center	gr.fire.fire_service.c2
France 112 Paris Department (231)	fr.112.112.dept231
France 112, Command & Control Center	fr.112.112.c2
Greek Olympia Odos Motorway	gr.motorway.olympia_odos
Greek Egnatia Odos Motorway	gr.motorway.egnatia_odos

4.1 Message recipients

The majority of message formats and communication protocols available worldwide use a "recipient" field to specify the recipient entity to which each message should be forwarded. This field should be populated by the EIP address of the communication nodes of the agencies to which each message will be forwarded.

Additionally, a set of predefined keywords has been reserved, in order to enable the message broadcasting to all nodes of an agency and the message forwarding only to the coordination centre of an agency.

For these purposes, the following two keywords are defined:

- .all - in order to send a message to all nodes of an organization
- .coordination - in order to send a message to the coordination centre of an organization

The keywords should be concatenated at the end of each agency's EIP address.

For examples, see Table 2.

Table 2 — Message recipients

Identity added to the recipient element of the message	Nodes of the organization that will receive the message
gr.fire.fire_service.all	All nodes of the Greek Fire Service agency
gr.fire.fire_service.coordination	The coordination center of the Greek Fire Service agency
it.law_enforcement.carabinieri.all	All nodes of the Italian Carabinieri agency
it.law_enforcement.carabinieri.coordination	The coordination center of the Italian Carabinieri agency

5 Emergency Name Service

5.1 General

Usually, agencies have more than one communication node, each of these being focused on different aspects of the operations and based on different standards, protocols and technologies. The big variation in the characteristics of the communication nodes that are available around the EU limits their ease of use and connection establishment. Additionally, the EIP addresses of the agencies should be known beforehand among the agencies, in order to be used for message exchange purposes during a crisis.

The Emergency Name Service (ENS) provides a central mechanism that enables the central hosting, indexing and automatic discovery of the communication nodes of all agencies that are available during a specific period of time. ENS will play the role of a central repository that will host and make available to other agencies all the details of each agency's communication nodes.

ENS consists of two main sub-services:

- The Registration service;
- The Discovery service.

5.2 Registration service

Each communication node has the responsibility to register with the ENS. An interface should be provided by the ENS, enabling the registration of the communication nodes along with their characteristics. Each communication node will be represented by the following set of characteristics:

- **EIP**: it contains the unique identifier that has been assigned to the specific node.
- **Descriptive Name**: it contains the full name of the node.
- **IP**: it contains the IP address of the communication node.
- **Standards/protocols**: it contains the set of standards and protocols that are supported by the node, e.g. EDXL, WMS etc.
- **Communication technologies**: it contains the set of communication technologies that are supported by the node, e.g. Message Broker, REST API etc.
- **Jurisdiction Area:** it contains the responsibility area of the specific communication node.

ENS should provide a REST POST interface that will enable this registration process. The REST endpoint should follow the following format:

https://xxx.xxx.xxx.xxx/ens/register

The message that will be posted per communication node should be in JSON format. Upon receiving a registration request, the registration service will check the validity of the information provided by the endpoint, e.g. whether the EIP has been pre-registered etc.

The following Table 3 contains an example of the registration message that should be used in order to register the communication node.

Table 3 — Registration message

Description	Register an communication node of the Hellenic Fire Service.
REST POST endpoint	https://xxx.xxx.xxx.xxx/ens/register

Message (JSON format)	{
	“**register**”:{
	“**eip**”:”gr.fire.fire_service”,
	“**descriptive_name**”:”Hellenic Fire Service”,
	“**ip**”:”xx.xx.xx.xx”,
	“**standards_protocols**”:[
	“ISO TR 22351:2015”
	],
	“**communication_technologies**”:[
	“KAFKA Message Broker”
	],
	“**jurisdiction_Area**”:”Greece”
	}
	}

Response (JSON format)	{
	"**registerResponse**": {
	"**response**": "SUCCESS",
	"**token**": "ae0a6a56-875a-443c-950d-cf65da2ec95b"
	}
	}

5.3 Discovery Service

The Discovery service enables the automatic discovery of the communication nodes that have been registered into the ENS. A dedicated REST interface should be provided, enabling the query of the registered communication nodes, using a set of characteristics. Thus, operations such as: *retrieve the EIP address of the Hellenic fire service* and *retrieve the communication points of all motorways in Greece*, should be covered.

ENS should provide a REST GET interface that will enable this discovery process. The REST endpoint should conform to the following format:

https://xxx.xxx.xxx.xxx/ens/discovery

The message that will be posted per query should be in JSON format. Each query message should contain a set of variables/characteristics that will be compared with the related variables/characteristics in the repository of ENS, in order to find the related communication nodes.

In case no communication node is detected, using the queried characteristics, the node field will be returned empty.

The following contains two examples of query messages and related responses:

Example 1:

An entity would like to communicate with the Hellenic Fire Service. The use of ENS Discovery service should be used, in order to retrieve the communication node and the related communication details.

The query message prepared and submitted to the following END Discovery service REST endpoint is:

```
{
  “query”:{
    “descriptive_name”:”Hellenic Fire Service”
   }
}
```

Upon the message submission, the Discovery service will search the repository for the specific description name. The response that will be prepared and returned to the query will have the following format:

```
{
  "queryresponse": {
   "response": "SUCCESS",
   "node": {
      “eip”:”gr.fire.fire_service”,
      “descriptive_name”:”Hellenic Fire Service”,
      “ip”:”xx.xx.xx.xx”,
      “standards_protocols”:[
         “ISO TR 22351:2015”
       ],
      “communication_technologies”:[
         “KAFKA Message Broker”
      ],
      “jurisdiction_Area”:”Greece”
     }
   }
  }
}
```

<u>**Example 2:**</u>

An entity would like to communicate with one of the main motorways of Greece: Egnatia Odos. However, as the exact descriptive name of this motorway may not be known beforehand, a recursive approach could be used. Initially using the ENS Discovery service, the retrieval of information about all communication nodes of motorways in Greece would be enabled. Then, the entity could filter the list of available nodes, in order to choose the final one for communication.

The query message was prepared and submitted to the following END Discovery service REST endpoint, in order to retrieve information about all communication nodes of motorways in Greece is:

```
{
  “query”:{
    “EIP”:”gr.motorway”
   }
}
```

Upon the message submission, the Discovery service will search the repository for the records that satisfy the specific EIP address. The response that will be prepared and returned to the query will have the following format:

```
{
 "queryresponse": {
  "response": "SUCCESS",
  "node": [{
    “eip”:”gr.motorway.olympia_odos”,
    “descriptive_name”:”Olympia Odos Motorway”,
    “ip”:”xx.xx.xx.xx”,
    “standards_protocols”:[“EDXL-CAP”],
     “communication_technologies”:[“REST API”],
     “jurisdiction_Area”:”Olympia Odos”
    }
   },{
    “eip”:”gr.motorway.egnatia_odos”,
    “descriptive_name”:”Egnatia Odos Motorway”,
    “ip”:”xx.xx.xx.xx”,
    “standards_protocols”:[ “EDXL-CAP”],
     “communication_technologies”:[ “REST API”],
     “jurisdiction_Area”:”Egnatia Odos”
    }
   }],
 }
}
```

The details of the communication nodes of two different motorways in Greece have been returned. Using this response, the entity can filter the information, selecting only the one that is required for communication.

Bibliography

[1] B.S. Manoj and Alexandra Hubenko Baker, "Communication challenges in emergency response," Communications of the ACM – Emergency response information systems: emerging trends and technologies, Vol. 50, No. 3, 2007, pp. 51-53. doi:10.1145/1226736.1226765

[2] https://www.statewatch.org/media/documents/news/2018/sep/eu-council-iss-implementation-draft-report-12009-18.pdf