CEN

WORKSHOP

AGREEMENT

CWA 17513

May 2020

English version

Crisis and disaster management - Semantic and syntactic interoperability

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

European foreword

This CEN Workshop Agreement (CWA 17513:2020) has been developed in accordance with CEN-CENELEC Guide 29 'CEN/CENELEC Workshop Agreements – The way to rapid consensus' and with the relevant provision of CEN/CENELEC Internal Regulations – Part 2. It was approved by a Workshop of representatives of interested parties on 2019-04-29,the constitution of which was supported by CEN following the public call for participation made on 2019-04-01. However, this CEN Workshop Agreement does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

Results incorporated in this CEN Workshop Agreement received funding from the European Union's 7th Framework Programme for Research, Technological Development and Demonstration under Grant Agreement (GA) N°607798 and N°607078. This CEN Workshop Agreement (CWA) is based on the results of the DRIVER+ and EPISECC research project. The final text of CWA 17513:2020 was submitted to CEN for publication on 2020-03-27.

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

— Austrian Institute of Technology GmbH/ Georg Neubauer, Maria Egly, Patrick Zwickl;

— Austrian Red Cross/ Thomas Seltsam;

— German Aerospace Center/ Angela Uschok;

— HITEC Luxembourg S.A./ Harold Linke;

— Public Safety Communication Europe Forum/ David Lund;

— Riskaware Ltd/ Robert Gordon;

— Netherlands Organization for Applied Scientific Research/ Erik Vullings;

— Frequentis AG/ Thomas Obritzhauser;

— SBA Research gGmbH/ Kevin Mallinger, Markus Klemen, Andreas Ekelhart;

— The Main School of Fire Service/ Tomasz Zwęgliński;

— Thales SIX GTS France SAS/ Laurent Dubost; and

— University of Split/ Snjezana Knezic, Martina Baucic.

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.

Introduction

Current and future challenges, due to increasingly severe consequences of natural disasters and terrorist threats, require the development and uptake of innovative solutions that are addressing the operational needs of practitioners dealing with crisis and disaster management. This document is based on the results of DRIVER+ and EPISECC and defines requirements on how to achieve organizational and cross border interoperability on semantic and syntactic level for crisis and disaster management.

DRIVER+ (Driving Innovation in Crisis Management for European Resilience) was a European research project funded under the 7th Framework Programme (FP7) that aimed to improve the way capability development and innovation management is tackled. EPISECC (Establish a Pan-European Information Space to enhance the Security of Citizens) on the other hand aimed to develop a concept of a common European information space.

DRIVER+ identified four capability gaps that specifically refer to operational interoperability:

— Exchanging crisis and disaster related information among agencies and organizations: Shortcomings in the ability to exchange relevant information among agencies and organizations, such as authorities, first responders and crisis managers.

— Common understanding of the information exchanged in response operations: Limits in the ability to ensure a common understanding of the information exchanged (terminology, symbology) by all crisis and disaster managers involved in response operations.

— Understanding crisis and disaster management capabilities of participating organizations: Lack of mutual knowledge or alignment of operational needs and procedures between different organizations responding to the same scenario.

— Shared awareness of status and planned efforts in crisis and disaster management operations: Insufficient understanding of the overall current and planned response efforts as well as current strategies across organizations during an event.

EPISECC identified similar gaps related to interoperability in line with the ones identified in DRIVER+. Information exchange between agencies and organizations involved in crisis and disaster management is of imperative relevance during all phases of the disaster management cycle. Especially in the response phase of a crisis or disaster exchange it is necessary to ensure adequate response to the triggering event. Information exchange between the involved agencies and organizations need to remain established under any conditions.

The communication between different organizations, regions and countries – with their specific processes and tools – is a major challenge in crisis and disaster management. Both efficient communication and access to critical information is a key requirement for the operation of public safety and security services, as well as in the preparation for and the management of crisis and disasters. The members of this CEN Workshop decided based on the above information to initiate this agreement.

1 Scope

This document defines requirements to achieve organizational and cross border interoperability on semantic and syntactic level for crisis and disaster management. The document provides syntactic requirements on the realization of tool connectors to a platform, standardized protocols, validation of transmitted messages, security issues, message distribution approaches and system resilience. Regarding semantic services recommendations on the establishment of semantic resources as well as the establishment of a semantic mapping and matching are given.

This document is dedicated to support both practitioners and solution providers in the process of the realization of interoperability between IT solutions designed for the application in the crisis and disaster management domain. Practitioners are people who are qualified or registered to practice a particular occupation in the field of security or civil protection, e.g. crisis managers and responders related to all disciplines of crisis and disaster management and response. Solution providers are those that develop and supply technological solutions that fulfil the requirements defined in this document, with the goal to improve operational capabilities of practitioners.

In addition, use cases for the application of syntactic and semantic services are given. Layer models are described and examples of concepts and topologies are provided.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

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

3.1
actor
role played by a user or any other system that interacts with the subject

Note 1 to entry: Part of the syntax of UML.

3.2
capability gap
gap between the current ability to provide a response and the actual response assessed to be required for a given threat or hazard

3.3
data entity
an entity that was declared to be data and therefore is not parsed when referenced

3.4
data model
graphical and/or lexical representation of data, specifying their properties, structure and inter-relationships