SLOVENSKI STANDARD
SIST-TS CEN/TS 18053-1:2024

01-november-2024

Digitalna skrbniška veriga za dokaze CBRNE - 1. del: Pregled in koncepti

Digital Chain of Custody for CBRNE Evidence - Part 1: Overview and Concepts

Digitale Beweiskette für CBRNE-Beweise - Teil 1: Überblick und Konzepte

Ta slovenski standard je istoveten z: **CEN/TS 18053-1:2024**

ICS:

13.300	Varstvo pred nevarnimi izdelki	Protection against dangerous goods
35.240.99	Uporabniške rešitve IT na drugih področjih	IT applications in other fields

SIST-TS CEN/TS 18053-1:2024 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 18053-1

September 2024

ICS 13.300; 35.240.99

English Version

Digital Chain of Custody for CBRNE Evidence - Part 1: Overview and Concepts

Digitale Beweiskette für CBRNE-Beweise - Teil 1: Überblick und Konzepte

This Technical Specification (CEN/TS) was approved by CEN on 26 May 2024 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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, Türkiye 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

Ref. No. CEN/TS 18053-1:2024 E

Contents

Page

European foreword

This document (CEN/TS 18053-1:2024) has been prepared by Technical Committee CEN/TC 391 *"Societal and citizen security"*, the secretariat of which is held by AFNOR.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: 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, Türkiye and the United Kingdom.

Introduction

In situations involving chemical, biological, radiological, nuclear, and explosive (CBRNE) incidents caused by natural or accidental events or deliberate actions like terrorism or warfare, it can be crucial to accurately identify CBRNE agents by collecting and transporting samples to a laboratory. A digital chain of custody system might contribute to ensuring the traceability and security of CBRNE evidence items throughout the process. This process involves various stakeholders, emphasizing the significance of maintaining the integrity of the chain of custody and documenting all actions, particularly at Custody Transfer Points (CTPs), for easy auditing of the involved stakeholders.

In any digital Chain of Custody (dCoC) process, it is essential to identify stakeholders with specific roles or participation in the dCoC process. These stakeholders may include the Mission Commander Team, the Reconnaissance Team, the Sampling Team, the Carrier Team, and the Laboratory Team. The data governance workflow aims to offer guidance on executing a secure digital transfer and identifying the stakeholders involved as contributors to the evidentiary materials at each stage of the process. The guidelines emphasize the importance of incorporating digital custody metadata (DCM) into the dCoC process to ensure the integrity and non-repudiation of digital evidence items and to trace the custodian. By including DCM, the dCoC process can provide comprehensive and accurate documentation of all steps involved in the custody, control, transfer, and auditing of the digital evidence items, thereby increasing transparency and accountability.

This document addresses services and final outputs concerning dCoC for CBRNE evidence items. The concepts and terminology presented in this document are utilized by the definitions in ISO 22095 Chain of Custody – General terminology and models. Additional definitions of concepts relevant to the CTP data governance process specification and custody transfer of metadata structures considered by the digital evidence log are also provided. Many of the terms and definitions listed here are also mentioned in the EN 17173 European CBRNE glossary; although not mandatory, reading these two standards is suggested to get familiarised with the terms and definitions listed for the chain of custody in the area of CBRNE.

The guidelines can be applied to other supply chains (e.g. food chains, retail logistics, etc.). The dCoC for CBRNE digital evidence items represents a paradigmatic context to address data governance considerations for evidentiary purposes in a highly demanding framework.

This document is intended to be used with Part 2 in order to ensure the implementation of the custody transfer data governance process. Part 2 provides the technical details regarding the implementation of the data structure for the DCM in each CTP in the dCoC.

NOTE 1 It is important to emphasize that across the European Union, there are several regulatory and legislative procedures to handle the chain of custody for CBRNE incidents, so it is essential to take these considerations into account. The use of the guidelines can vary based on the digital evidence procedures adopted in each member state of the European Union.

NOTE 2 If the digital log for each custody transfer (i.e. who owns the custody at each transfer point) is not preserved, the evidence submitted in the court might be challenged and ruled inadmissible.

1 Scope

This document provides an overview of the concept of Custody Transfer Point (CTP) within the digital Chain of Custody (dCoC) process, including the identification and audit of the custody ownership and metadata governance to ensure the integrity of the data at each CTP. The document also provides:

- Definitions of the concepts within the dCoC process related to the digital evidence log for each custody transfer (i.e. who owns the custody at each transfer point);
- General guidelines for the data governance process within the CTP lifecycle, including identification of the role of the stakeholders;
- Digital metadata management policies and compliance with good practices for non-repudiation of the reported data regarding the ownership of digital evidence items within the custody transfer lifecycle.

This is part one of two documents for the provision of Digital Custody Metadata (DCM) for managing data related to the custody of digital evidence items. Part 2 complements this document by providing detailed guidance on the steps in the data governance process within each CTP lifecycle.

The document aims to provide guidance to both technical and non-technical personnel, including individuals accountable for compliance with statutory and regulatory requirements and industry standards. It is designed to be helpful for a broad range of professionals, regardless of their technical expertise, ensuring that all stakeholders involved in implementing the document's recommendations can understand and follow them effectively.

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:

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

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

3.1
audit
process for obtaining relevant information about an object of conformity assessment and evaluating it objectively to determine the extent to which specified requirements are fulfilled

[SOURCE: ISO 22095:2020, 3.5.6]

3.2
authorised custody carrier
person or entity which arranges transportation of digital evidence items, on its own behalf or on behalf of others, in their name or on its own, even if using the means of others, responsible for the staff, vehicles and structures which are made available

[SOURCE: EN 17173:2020, 3.33, modified by removing “radioactive material”.]

3.3
concern
matter of interest or importance to the stakeholder

3.4
custody transfer point
concept that documents and maintains a chronological history of digital information about the custody transfer instant for a specific mission; part of the dCoC process (represented by a node in the dendrogram), where the custodianship is transferred from one authorized custody carrier to another

Note 1 to entry: Provides a non-repudiation log with undauntable details on the point at which the evidence item is defined as being delivered or loaded.

3.5
data governance
workflow focused on managing the quality, consistency, usability, security, and availability of information, together with the governance checkpoint processes to show continued compliance monitoring

Note 1 to entry: It includes setting policies that apply to how data are gathered, stored, processed, and disposed of. It governs who can access what kinds of data are under governance.

Note 2 to entry: This process is closely linked to data ownership and stewardship notions.

Note 3 to entry: Data governance also involves complying with external standards - data policies - set by industry associations, government agencies, and other stakeholders.

3.6
digital chain of custody
non-repudiation digital record with verifiable information about the possession, movement, handling, and location of digital evidence items from one point in time until another

Note 1 to entry: A process by which inputs and outputs and associated information are digitally transferred, monitored and controlled as they move through each CTP.

[SOURCE EN 17173:2020, 3.96, modified by focusing on tracking metadata related to the custodianship of digital evidence items.]

3.7
digital custody metadata
data model that defines and describes data related to the custodianship and custody transfer of CBRNE digital evidence items

Note 1 to entry: Metadata may describe data, data elements, or other objects.

Note 2 to entry: Metadata may include data descriptions, data about data ownership, measurements, indicators, access paths, access rights, data volatility or any other information digitally provided.

[SOURCE: ISO/IEC 11179-1:2015, 3.2.16, modified by focusing the metadata structure on custodianship at each CTP.]

3.8
digital chain of custody process
abstract description of a digital chain of custody (3.5) representing a sequence of custody transfer actions with a generic set of parameters to monitor the execution of the information flow within the digital chain of custody

Note 1 to entry: A workflow can be used to map out the execution of a custody transfer point (3.3) from its starting point to its outcome.

3.9
digital evidence item
detailed digital information stored or transmitted in binary form that may be relied on as evidence

Note 1 to entry: Unlike physical evidence, it can be altered or deleted remotely.

Note 2 to entry: Provides actionable intelligence on the status of the evidence information at every point in time and presents the findings for prosecution

Note 3 to entry: Stakeholders need to be able to authenticate the digital evidence and also provide additional information to prove its integrity.

Note 4 to entry: A digital evidence item may refer to a physical sample and/or to a data measurement.

3.10
digital non-repudiation log
secure transaction log file with information that can't be denied as having taken place or being legitimate

3.11
digital twin evidence
digital representation of a physical evidence item, corresponding to a data model characterising a physical evidence item or data measurement within a chain of custody process

3.12
custodian owner
stakeholder (i.e., person or information system) that has a custody, control or possession of data regarding a digital evidence (3.8) item

Note 1 to entry: A custodian owner is defined as the resource that, at the moment, directly holds the custodianship of a specific digital evidence item.

Note 2 to entry: From an information system perspective, databases and applications, network storage and digital archives can also be considered a custodian resource.

3.13
custodian receiver
stakeholder that assumes the custodianship of data regarding a digital evidence (3.8) item

Note 1 to entry: This can be a person or information system

3.14
metadata
data that provides descriptive information about other data

Note 1 to entry: Metadata should be used to discover and characterize data artefacts within the digital chain of custody (3.5).

3.15
mission
unique reference to an event requiring the implementation of a formal data governance process coordinated by a mission command team

Note 1 to entry: Action-based statement with a set of metadata (3.13) identifying the purpose of a specific event.

3.16
mission resource
resource assigned to accomplish a specific task in the mission (3.14) and which is coordinated under a mission command team

Note 1 to entry: A resource can be a person, equipment or any informational system used to accomplish a specific task in the assigned mission

3.17
verification
confirmation of truthfulness through the provision of objective evidence that specified requirements have been fulfilled

Note 1 to entry: The objective evidence needed for verification can result from an inspection, audit or other forms of determination, such as performing alternative calculations or reviewing documents.

Note 2 to entry: The word “verified” is used to designate the corresponding status.

[Source: ISO 22095:2020 Chain of custody, 3.5.8 verification]

4 Symbols and abbreviated terms

AAA	Authentication, Authorization, and Accounting (or Auditing)
API	Application Programming Interface
CIA	Confidentiality, Integrity and Availability
CTP	Custody Transfer Point
DO	Data Object
dCoC	digital Chain of Custody
DCM	Digital Custody Metadata
GUI	Graphical User Interface

NFC	Near Field Communication
SOP	Standard Operating Procedures
STS	Security Token Service
ROV	Remotely Operated Vehicle

5 General Guidance

5.1 General

The flow of information in a typical chain of custody process is primarily done through paper documents [1]. When creating a digital twin of this process, the rules for ensuring the authenticity and integrity of digital data used for evidentiary purposes should be similar. Guidance should be provided on what metadata to apply in the digital environment, especially when it is necessary to keep track of who has custody of digital evidence at each handover point.

The purpose of the custody transfer point (CTP) is to encapsulate and protect information related to digital evidence that needs to be transferred between two locations by mission resources. Digital custody metadata (DCM) provides the metadata to characterize each CTP within the digital chain of custody (dCoC) process. Because DCM often involves collecting sensitive data, it may be privacy-invasive. Therefore, these guidelines are also intended to help ensure compliance with data protection aspects.

This section steers the dCoC process by providing stakeholders with guidelines to set up a practical and reliable DCM audit and identify those involved in the custody transfer lifecycle. These guidelines aim to establish rules for implementing CTP actions to ensure admissible integrity and ensure the chain of evidence in administrative, disciplinary and judicial proceedings.

5.2 Background context

Maintaining the chain of custody is about preserving the integrity of the information in the digital custody metadata (DCM). A consistent data governance workflow provides a trackable digital fingerprint regarding the digital evidence item collected at the site scene and that it is in its original/unaltered state [2].

DCM should be trustworthy, with little or no possibility for manipulation or human interaction. However, data are easily transported, so data governance and uniformisation of metadata describing who owns the custody at each CTP is required, such that:

- the dCoC consists of recording metadata information and access control and security issues for all digital handlings in the process;
- the dCoC is also a chain of responsibility for the custodianship of digital evidence items as they move through each CTP;
- during the dCoC process, the purpose is to ensure that the data claimed for a specific digital evidence item are indeed the ones that are delivered in the output;
- the dCoC can use traceability records to identify the stakeholders that take legal ownership or physical control over a specific digital evidence item;
- keeping a standardized record of the DCM is a critical issue, as the authenticity of metadata evidence should be maintained (for further details on the DCM data model, please see Part 2);
- following a standardized process to ensure data quality within the dCoC is essential (for more information, please see Part 2).