SLOVENSKI STANDARD
SIST-TS CEN/TS 18053-2:2024

01-november-2024

Digitalna skrbniška veriga za dokaze CBRNE - 2. del: Upravljanje podatkov in presoja

Digital Chain of Custody for CBRNE Evidence - Part 2: Data Management and Audit

Digitale Beweiskette für CBRNE-Beweise - Teil 2: Datenmanagement und Audit

Ta slovenski standard je istoveten z: **CEN/TS 18053-2:2024**

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 18053-2:2024 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 18053-2

September 2024

ICS 13.300; 35.240.99

English Version

Digital Chain of Custody for CBRNE Evidence - Part 2: Data Management and Audit

Digitale Beweiskette für CBRNE-Beweise - Teil 2: Datenmanagement und Audit

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

Contents

Page

European foreword

This document (CEN/TS 18053-2:2024) has been prepared by Technical Committee CEN/TC 391 “Societal and citizen security”, the secretariat of which is held by AFNOR.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

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

This document presents the metadata that should be considered for automating the custody transfer of digital evidence items within a digital Chain of Custody (dCoC). The goal is to provide guidelines for a standardized metadata structure for auditing the custody transfer between stakeholders. These guidelines intend to support data integrity and to ensure compliance with business rules in each custody transfer point (CTP).

The proposed data structure is designated as Digital Custody Metadata (DCM). It is an essential tool for auditing the data governance workflow, providing a digital log with information about who has custody and how that custody was transferred between stakeholders. Such information should be admissible in administrative, disciplinary, and judicial proceedings. If a digital log of each custody transfer is not preserved, the evidence presented in court may be challenged and ruled inadmissible. Therefore, the goal is to provide guidelines for a non-repudiation digital log, ensuring a standard data structure for data management and auditing.

In order to understand who holds a CBRNE digital evidence item within each CTP lifecycle, the DCM should provide comprehensive information. This information encompasses details about the location and timing of the custody transfer, identification of the custody owner and receiver, and metadata about the package used for transporting the digital evidence items. Additionally, the DCM should provide insights into the status of the CTP, including information about successfully executed CTPs and triggers for situational awareness.

In this domain, actions related to situational awareness that necessitate the involvement of the Mission Command Team or pertain to suspicious situations potentially jeopardising the integrity of the DCM should be highlighted. These actions warrant specific instructions on how to proceed with the custody transfer. In such instances, the CTP dendrogram should clearly outline the particular CTP node that triggered the alert.

This document focuses on the CBRNE digital evidence item transport lifecycle, from collection to its final destination. Sample collection techniques, preservation and packaging procedures are outside the scope of this document as they are well documented in existing standards. A well-documented dCoC should be established through a data governance process and with guidelines to ensure the integrity of the DCM for each CTP in the dCoC process.

This Part 2 should be considered alongside with Part 1 - Overview and concepts. Together with Part 1 - Overview and concepts - it is possible to obtain a complete understanding of the custody transfer lifecycle.

1 Scope

This document provides guidelines for managing and auditing Digital Custody Metadata (DCM), enabling stakeholders to identify and audit custody ownership for CBRNE digital evidence items in the digital chain of custody (dCoC). It proposes a metadata structure to manage resources assigned to a CBRNE mission and comply with good data governance practices, raising awareness at each custody transfer point.

The information flow within the dCoC is modelled using the Business Process Model and Notation (BPMN) to specify the DCM governance workflow. This standard notation provides a formal representation that helps understand the challenges associated with the DCM. The goal is to focus on the metadata structures required to manage digital asset custodians while outlining the data to be considered when specifying a DCM governance workflow.

This document is the second part of two Technical Specifications (TS) on the provision of DCM services for managing data related to the custody of CBRNE digital evidence items.

2 Normative References

There are no normative references in this document.

3 Terms and Definitions

No terms and definitions are listed in this document.

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

4 Symbols and Abbreviated Terms

AAA	Authentication, Authorization, and Accounting
API	Application Programming Interface
CC	Command Centre
CTP	Custody Transfer Point
dCoC	digital Chain of Custody
DCM	Digital Custody Metadata
GUI	Graphical User Interface
ICT	Information and Communications Technology
KPI	Key Performance Indicator
RAV	Remote Aerial Vehicle
RGV	Remote Ground Vehicle
ROV	Remotely Operated Vehicle
TS	Technical Specification
UX	User Interface

5 Data Governance in the Digital Custody Transfer Domain

5.1 General

This section provides guidelines for implementing data verification measures, guaranteeing their availability, integrity, authentication, confidentiality, and non-repudiation. These measures serve the purpose of creating a digital evidence log, documenting custodianships and the transfer of digital custody between stakeholders. The digital log constitutes an information assurance storage, enabling auditing of the data governance workflow while ensuring integrity checks are in place.

Those responsible for data governance, particularly those who need to analyse metadata characterizing the digital evidence, should seek to create:

- A culture that considers DCM as a valuable digital asset, being accountable for ensuring that legal, ethical, and other requirements comply;

- Assure that all DCM are harmonized and adequately stored in an evidence log, with the possibility to query the chronological execution of custody transfer transactions;

- All parties involved in developing policy, planning and implementation should know the causes of failure associated with DCM processes, their responsibilities, and potential mitigation actions.

Management support is also essential for successfully establishing, implementing, maintaining and continually improving the DCM process. Management should evaluate existing policies and demonstrate leadership and commitment to mitigate uncertainty [1]. The goal is to provide a reliable data governance workflow for each CTP lifecycle.

Figure 1 illustrates that the DCM process is organized into three levels of metadata governance. Maintaining an appropriate balance between controls and management should be considered for effective communication with all stakeholders involved in the CBRNE mission. Additionally, any situational-awareness actions requiring the intervention of the Mission Command Team or associated with suspicious situations that could potentially compromise the integrity of the DCM should be flagged for in-depth analysis. These situations should be communicated to all stakeholders, including operational decision-makers, to enhance awareness and accountability.

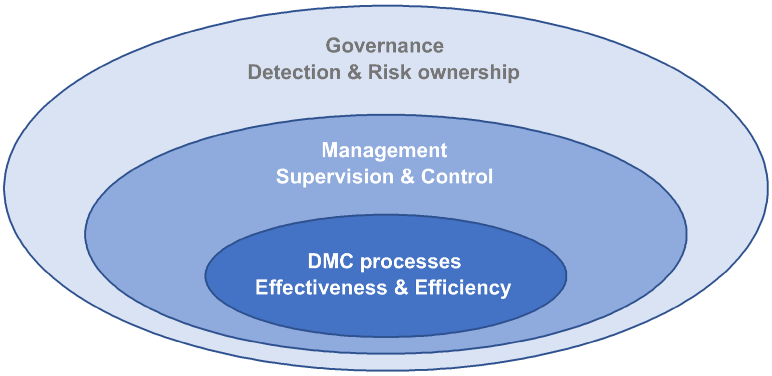

Figure 1 — Metadata governance harmonization

Those responsible for metadata harmonization should ensure that DCM processes are controlled according to the risk criteria and conform to the specified guidelines:

- Promote a shared understanding of various concepts and terminology for the governance of DCM processes from the viewpoint of the intervenient stakeholders (i.e. different Teams in the dCoC);
- Articulate objectives and structures for digital metadata governance;
- Encourage a practical and cost-effective establishment of DCM processes;
- Provide guidance and best practices to those responsible for executing DCM strategies and policy;
- Identify tasks and strategy contexts for the metadata governance so that it may help in setting policy and design controls, suggesting ways to avoid adverse effects on reputational factors;
- Promote the proactive use of metrics and risk evaluation practices for minimizing failure in the DCM processes;
- Provide guidance for compliance, conformance and effectiveness review.

The overriding goal is to help organisations establish good data governance practices for their DCM processes. Setting up a data governance structure for cross-border functioning and mechanisms for a coordinated approach between stakeholders helps establish a global and harmonized view of the DCM. The guidelines also foster the need for cooperation and interoperability between third-party systems to deliver DCM services seamlessly.

5.2 The Data Governance Process

Data governance allows setting and enforcing controls that would enable greater access to data, gaining security and privacy from the controls on data. Data governance ensures that data are safe, secure, private, usable, and compliant with internal and external data policies [2]. It ensures that data are consistent and trustworthy and does not get misused. Another data governance goal is to ensure data are used correctly, blocking potential misuse of sensitive information [3]. That can be accomplished by creating uniform data policies on the use of data, along with procedures to monitor usage and enforce the policies continuously.

The data governance policies should be developed, along with rules that define how data can be used by authorized personnel [4]. In addition, controls and audit procedures are needed to ensure ongoing compliance with internal policies and external regulations and guarantee that data are used consistently across applications.

In the DCM governance workflow, it is essential to be aware of and mitigate specific causes of failure which can compromise the dCoC. The DCM governance workflow aims to avoid negative consequences, including those described below:

- Breaches of privacy caused by inappropriate methods or accidental/non-compliance disclosure;
- Original damage to DCM caused by improper methods, including the damage to data integrity, authenticity, reliability or usability; and any other potential causes of spoliation;
- Inconsistency in the data structure caused by inappropriate disclosure to any third parties;
- Damage or non-compliant management of the evidence chain can render the DCM inadmissible in court.

These risk assessments prevent or reduce undesirable effects and deliver continuous improvement. It requires an evaluation of the internal and external context (including business, legal and jurisdictional issues, and ICT infrastructure).

In addition to the risk assessment, metrics for monitoring the execution of DCM processes have to be established. These metrics should monitor progress and compliance with defined requirements to ensure the expected outcomes within the dCoC process. Appropriate use of metric-based monitoring can indicate whether particular targets (e.g. critical dates or who owns the custody at each CTP) are likely to be met. Consultations with the external parties and the stakeholders that can be adversely affected by the DCM processes can help set the metrics.

In a CTP, multiple entities may access digital evidence items during the dCoC process. Therefore, when managing digital evidence, it is relevant to know who owns the custodianship of what digital evidence [5]. Consequently, for each CTP, the DCM should provide the following:

- **Integrity**, the digital evidence has not been altered or corrupted during the transfer.
- **Traceability**, the digital evidence should be traced from the time of its collection until it is destroyed.
- **Authentication**, all the resources (e.g. authorized stakeholders and equipment) interacting with the digital evidence should provide irrefutable and recognizable proof of their identity.
- **Verifiability**, the data governance process should be verifiable by every stakeholder involved.
- **Security**, changeovers of digital evidence cannot be altered or corrupted.

The evidence log should provide integrity checks (i.e. every CTP can verify and detect if there has been an integrity breach that would invalidate the digital evidence transfer). A smart contract to keep track of ownership changes should be implemented for the dCoC (see Part 1 for more information about smart contracts).

5.3 The Custody Transfer Lifecycle

The CTP is a vital element within the DCM process. It is designed to ensure verifiable integrity and traceability of ownership. To achieve this, the CTP involves the active participation of two role-assigned Resources: the custody owner and the custody receiver. Both Resources are required to acknowledge the DCM information to complete a custody transfer successfully.

If only one of the Resources acknowledges the data, it triggers a non-conformity situation. Consequently, the system assesses the risk level and prompts the user to provide a comment identifying the detected inconsistency in the DCM. This triggers the need to abort the normal execution of the custody transfer. In such cases, custody is assumed temporarily to ensure the packet's delivery to the next CTP. Since digital evidence can be compromised during this period, analysing it as soon as possible should be a priority.

Figure 2 provides a high-level view of the data governance process [6] that should be performed for each CTP. The data verification process includes the following aspects:

- Validate the CTP data regarding the assigned CBRNE mission;
- Validate the package data, including the data describing the sample bags that the package holds;
- Validate the Resources data, meaning verify the data relating to the custody owner and receiver.

If an inconsistency or any other suspicious situation is identified in the reported information within the DCM, there is a potential risk of unauthorised data alteration. The Mission Command Team should be informed regarding this situation so that they can provide appropriate instructions on the next course of action. The data governance process of the CTP should include mechanisms to report such situations and reject the custodianship of the CTP. The CTP data governance process presented in Figure 2 maps the two possible use cases:

- Use Case 1: if no data inconsistency is reported (Figure 2.a), the CTP is successfully completed. In this case, the DCM should be updated to reflect the new custody owner. This updated information should be visually represented in the CTP dendrogram, allowing the Mission Command Team to verify the successful execution of the CTP easily.

- Use Case 2: in the event of a reported data inconsistency (Figure 2.b), the CTP is not successfully completed, and an alert should be promptly sent to the Mission Command Team. They can then analyse the reported inconsistencies and provide instructions on how to proceed with the custody transfer. At this point, to prevent disruption of the dCoC, custody is conditionally assumed until the package reaches its final destination or until an intermediate Laboratory Team assesses the impact of the reported inconsistency.

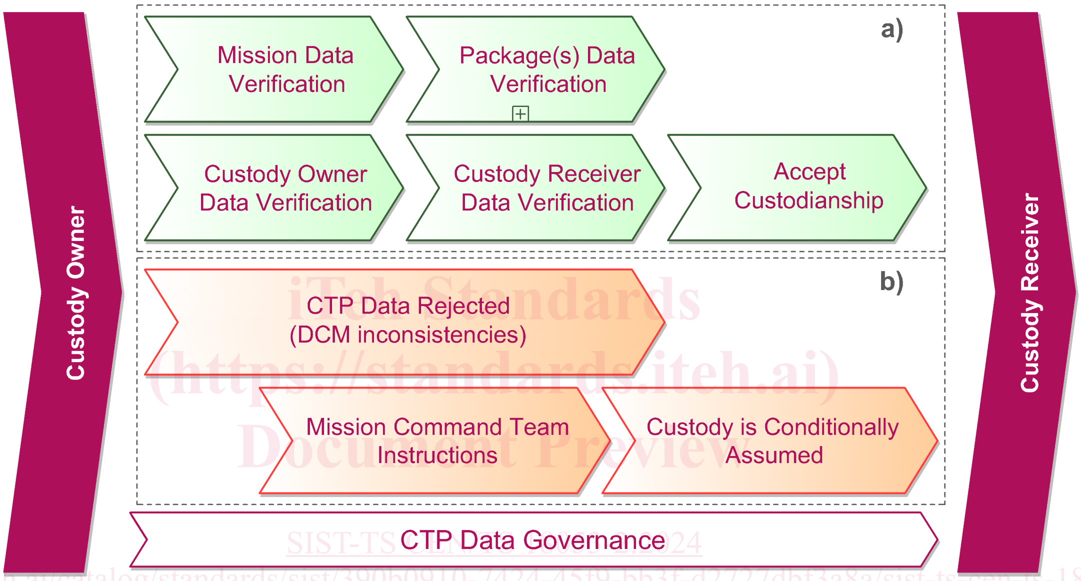
Custody Owner
a)
Mission Data Verification
Package(s) Data Verification
Custody Owner Data Verification
Custody Receiver Data Verification
Accept Custodianship
b)
CTP Data Rejected (DCM inconsistencies)
Mission Command Team Instructions
Custody is Conditionally Assumed
CTP Data Governance
Custody Receiver

Figure 2 — High-level view of the CTP data governance process

A data inconsistency should be reported whenever the information in the DCM for the corresponding CTP is not validated by one of the assigned Resources (i.e. custody owner or custody receiver). The CTP node in the dendrogram should be displayed as unsuccessful, and the Mission Command Team should be notified to provide instructions on how to proceed. As presented in Table 1, the severity level for a data inconsistency should be indicated in the alert message.