

ISO/IEC JTC 1 N 9481
ISO/IEC JTC 1
Information Technology

2009-01-20

Document Type: Proposed NP

Document Title: SC 27 Proposal for a new work item on guidelines for identification, collection and/or acquisition and preservation of digital evidence

Document Source: SC 27 Secretariat

Reference:

Document Status: This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 27 Secretariat.

Action ID: ACT

Due Date: 2009-04-20

No. of Pages: 10



ISO/IEC JTC 1/SC 27 **N7183**

ISO/IEC JTC 1/SC 27/WG 4 **N47183**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: proposed NP

TITLE: **Proposal for a new work item on guidelines for identification, collection and/or acquisition and preservation of digital evidence**

SOURCE: Secretariat of JTC 1/SC 27

DATE: 2009-01-14

PROJECT:

STATUS: In accordance with resolution (contained in SC 27 N6904) of the 5th SC 27/WG 4 Plenary meeting held in Limassol (Cyprus), 6th – 10th October 2008, this document is being circulated to the SC 27 National Bodies for a 3-month NWIP letter ballot and to JTC 1 for a concurrent review.

P-Members of SC 27 are requested to submit their votes on this document via the ISO e-balloting application by **2009-04-14**.

Secretariat's note: SC 27/WG 4 would like to express its appreciations to the National Bodies of Malaysia, Australia and United States for making available to SC 27 such a valuable contributions to WG 4's Study Period on acquisition procedure (as presented in SC 27 N7002rev1) that resulted in producing this NWIP (see SC 27 N7183) which is mainly based on the Malaysian contribution (see Attachment 2 of N7002rev1).

ACTION ID: LB

DUE DATE: 2009-04-14

DISTRIBUTION: P- and L-Members
L. Rajchel, JTC 1 Secretariat
K. Brannon, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-chair
E. J. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenber, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 9

New Work Item Proposal

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2008-10-08	Proposer: ISO/IEC JTC 1 SC 27
Secretariat: ISO/IEC JTC 1/SC27 DIN, Germany	ISO/IEC JTC 1/SC 27 N7183

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title: Information technology – Security techniques – Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Scope:

This International Standard will provide guidance concerning identification, collection and/or acquisition, marking, storage, transport, and preservation of digital evidence. This standard will cover acquisition of digital evidence from various types of sources including, but not limited to:

- static data sources
- data in transit (e.g. over networks)
- volatile data sources (e.g. mobile phones)

Notes:

This scope uses the term “digital evidence” to mean information that meets the requirements of the relevant jurisdiction for use in legal proceedings. As the standard is developed, care will be taken to use terminology that is not limited to a particular jurisdiction or purpose.

This scope does not include matters pertaining to analysis of digital evidence, or admissibility, weight, relevance, and other judicially-controlled limitations on the use of digital evidence in courts of law.

The proposed international standard will not mandate the use of particular tools or methods.

Annex 1 gives an indicative structure for the proposed international standard.

Purpose and justification:

Cross-border investigation is critical in this time where international boundaries have little effect on flows of digital information. Money and information are routinely and often instantaneously electronically transferred across countries and continents.

Recent international initiatives, such as the Convention on Cybercrime, demonstrate that the international community recognizes the importance of improved and shared digital evidence best practices.

An important need that will be met by the proposed international standard is the facilitation of inter-jurisdictional exchange of evidence.

This proposed international standard will provide benefits by reducing the requirement for expensive and time-consuming travel by investigative agency staff and witnesses. It will provide a basis for resolving disputes concerning digital evidence in legal proceedings.

This international standard will meet needs of people associated with:

- law enforcement and criminal proceedings;
- civil legal proceedings; and
- taking action within organizations when circumstances arise that require evidence to be collected, acquired, stored, preserved, or transported.

This proposed international standard complements ISO/IEC 27001 and ISO/IEC 27002, and in particular the control requirements concerning digital evidence acquisition by providing additional implementation guidance. In addition the standard will have applications in contexts independent of ISO/IEC 27001 and ISO/IEC 27002.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?

- ☒ a single International Standard
☐ more than one International Standard (expected number:)
☐ a multi-part International Standard consisting of parts
☐ an amendment or amendments to the following International Standard(s)
☐ a technical report , type

And which standard development track is recommended for the approved new work item?

- ☒ a. Default Timeframe
☐ b. Accelerated Timeframe
☐ c. Extended Timeframe

Relevant documents to be considered

Contributions received in the Study Period (SC 27 N7002 Rev 2 and SC 27 N7067)

Co-operation and liaison

Liaisons will be established with organizations already developing standards and best practices for digital evidence such as:

1. FIRST
2. ASCLAD
3. HTCIA

Preparatory work offered with target date(s)

Target dates

WD 2009-07 CD 2010-07 FDIS 2011-07 IS 2012-06

Signature: ISO/IEC JTC 1/SC 27 Secretary

Will the service of a maintenance agency or registration authority be required: No
- If yes, have you identified a potential candidate?
- If yes, indicate name

Are there any known requirements for coding? No

-If yes, please specify on a separate page

Does the proposed standard concern known patented items? No
- If yes, please provide full information in an annex

Are there any known accessibility requirements and or dependencies (see:
<http://www.jtc1access.org>)? No
- If yes, please specify on a separate page

Are there any known requirements for cultural and linguistic adaptability? No
- If yes, please specify on a separate page

Comments and recommendations of the JTC 1 or SC 27- attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon:
It is proposed to assign this new item to JTC 1/SC 27

Voting on the proposal - Each P-member of the ISO/IEC/JTC 1/SC 27 has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation:
2009-01-14

Closing date for voting:
2009-04-14

Signature of Secretary:
Krystyna Passia
Secretariat of JTC 1/SC 27

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	Validity	Explanation
A. Business Requirement		
A.1 Market Requirement	Essential <input checked="" type="checkbox"/> Desirable _____ Supportive _____	There is a generally accepted need for guidelines to facilitate the exchange of digital evidence between jurisdictions. The proposed standard also supports users of ISO/IEC 27001 and ISO/IEC 27002 by providing additional guidance on requirements concerning evidence acquisition.
A.2 Regulatory Context	Essential _____ Desirable _____ Supportive <input checked="" type="checkbox"/> Not Relevant _____	This standard supports regulatory needs where criminal or civil legal proceedings may be involved.
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes _____ No <input checked="" type="checkbox"/>	This is a new area of international standardization.
B.2 Commitment to other organization	Yes _____ No <input checked="" type="checkbox"/>	
B.3 Other Source of standards	Yes _____ No <input checked="" type="checkbox"/>	Other organizations do work relevant to some of the aspects of this proposal. Liaison will be established with those that meet ISO/IEC criteria for liaison organizations. However, there is no known source of standards similar to the proposed standard.
C. Technical Status		
C.1 Mature Technology	Yes <input checked="" type="checkbox"/> No _____	The concepts associated with this standard are mature. However, the standard will not be standardizing any particular technology; i.e. it is technology neutral.
C.2 Prospective Technology	Yes _____ No <input checked="" type="checkbox"/>	The proposed standard is technology neutral.
C.3 Models/Tools	Yes _____ No <input checked="" type="checkbox"/>	
D. Conformity Assessment and Interoperability		

D.1 Conformity Assessment	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	The proposed standard will not mandate the use of particular methods or tools for specific purposes, so conformity assessment is not appropriate.
D.2 Interoperability	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
E. Adaptability to Culture, Language, Human Functioning and Context of Use		
E1. Cultural and Linguistic Adaptability	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	The proposed standard will be internationally applicable and will not include requirements that limit its applicability in any cultural or linguistic context.
E.2 Adaptability to Human Functioning and Context of Use	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	The proposed standard will be able to be used by the intended target audience without the need for special provisions for diverse human functioning and diverse contexts of use.
F. Other Justification	Nil	

Notes to Proforma

A. Business Relevance. That which identifies market place relevance in terms of what problem is being solved and or need being addressed.

A.1 Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.

A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.

B. Related Work. Aspects of the relationship of this NP to other areas of standardisation work shall be identified in this section.

B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.

B.2 External Commitment. Groups, bodies, or for a external to JTC 1 to which a commitment has been made by JTC for Co-operation and or collaboration on this NP shall be identified here.

B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC 1 as PAS, they shall be identified here.

C. Technical Status. The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.

C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardisation.

C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.

C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.

D. Conformity Assessment and Interoperability

D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.

D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan

E. Adaptability to Culture, Language, Human Functioning and Context of Use

NOTE: The following criteria do not mandate any feature for adaptability to culture, language, human functioning or context of use. The following criteria require that if any features are provided for adapting to culture, language, human functioning or context of use by the new Work Item proposal, then the proposer is required to identify these features.

E.1 Cultural and Linguistic Adaptability. Indicate here if cultural and natural language adaptability is applicable to your project. If so, indicate how it is addressed in your project

plan. ISO/IEC TR 19764 (Guidelines, methodology, and reference criteria for cultural and linguistic adaptability in information technology products) now defines it in a simplified way:

“ability for a product, while keeping its portability and interoperability properties, to:

- be internationalized, that is, be adapted to the special characteristics of natural languages and the commonly accepted rules for their use, or of cultures in a given geographical region;
- take into account the usual needs of any category of users, with the exception of specific needs related to physical constraints”

Examples of characteristics of natural languages are: national characters and associated elements (such as hyphens, dashes, and punctuation marks), writing systems, correct transformation of characters, dates and measures, sorting and searching rules, coding of national entities (such as country and currency codes), presentation of telephone numbers and keyboard layouts. Related terms are localization, jurisdiction and multilingualism.

E.2 Adaptability to Human Functioning and Context of Use. Indicate here whether the proposed standard takes into account diverse human functioning and diverse contexts of use. If so, indicate how it is addressed in your project plan.

NOTE:

1. Human functioning is defined by the World Health Organization at <http://www3.who.int/icf/beginners/bg.pdf> as:
<<In ICF (International Classification of Functioning, Disability and Health), the term functioning refers to all body functions, activities and participation.>>
2. Content of use is defined in ISO 9241-11:1998 (Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability) as: <<Users, tasks, equipment (hardware, software and materials), and the physical and societal environments in which a product is used.>>
3. Guidance for Standard Developers to address the needs of older persons and persons with disabilities).

F. Other Justification Any other aspects of background information justifying this NP shall be indicated here

Annex – Indicative structure for the proposed standard

1.0 Scope

1.1 Audience

2.0 Normative references

3.0 Terms and definitions

4.0 General Principles

5.0 Abbreviations

6.0 Overview

7.0 Identification of Evidence

8.0 Collection of Digital Evidence

9.0 Acquisition of Digital Evidence

10.0 Packaging and Transporting of Digital Evidence

11.0 Preservation of Digital Evidence

12.0 Chain of Custody