

# **ISO/IEC JTC 1/SC 22/WG23 N 0253**

*Draft New Work Item Proposal: Software Code Signing*

**Date** 6 May 2010

**Contributed by** Larry Wagoner

**Original file name** NWIP code signing 05062010.doc

**Notes**

# New Work Item Proposal

February 2004

## PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2010-04-26	Proposer: SC22 WG23
Secretariat: ANSI (US)	<b>ISO/IEC JTC 1 N XXXX</b> ISO/IEC JTC 1/SC 22 N XXX

**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** - to be completed by the proposer.

<p><b>Title</b> (subject to be covered and type of standard, e.g. terminology, method of test, performance requirements, etc.) Information Technology -- Programming languages, their environments and system software interfaces -- Software Code Signing</p>
<p><b>Scope</b> (and field of application) This new work item encompasses the signing of software code and software executables.</p>
<p><b>Purpose and justification</b> - attach a separate page as annex, if necessary</p> <p>Digital signatures for software code are an important technique to ensure trustworthiness and integrity of the software. With a digital signature, there is a reliable way of verifying that what is being used hasn't been modified somewhere in the supply chain. This can have serious consequences for systems that are intended to implement integrity properties such as safety, security or privacy. For less critical systems, the use of a reliable capability to digitally verify software can deny access to attackers or prevent other forms of electronic vandalism.</p> <p>This project will provide a uniform way to digitally sign software so that the software can be verified at any stage between source and actual use. Code signing can apply to entire software programs, software libraries or to just code segments. Code signing will ultimately provide the needed basis for a widely used infrastructure to lessen the possibility of a supply chain attack.</p>
<p><b>Programme of work</b></p> <p>If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?</p> <p><input type="checkbox"/> a single International Standard</p> <p><input type="checkbox"/> more than one International Standard (expected number: ..... )</p> <p><input type="checkbox"/> a multi-part International Standard consisting of ..... parts</p> <p><input type="checkbox"/> an amendment or amendments to the following International Standard(s) .....</p> <p><input checked="" type="checkbox"/> a technical report , type .....2.....</p> <p>And which standard development track is recommended for the approved new work item?</p> <p><input checked="" type="checkbox"/> a. Default Timeframe</p> <p><input type="checkbox"/> b. Accelerated Timeframe</p> <p><input type="checkbox"/> c. Extended Timeframe</p>

**Relevant documents to be considered**

- The programming language standards of ISO/IEC JTC 1/SC 22.
- For market reasons, the specifications of popular languages that are not the subject of ISO standards.
- The software engineering standards of ISO/IEC JTC 1/SC 7, as a source of extra-linguistic mitigation methods.
- The crypto standards of ISO/IEC JTC1/SC27
- Java Archives (JAR) File Specification
- Microsoft Authenticode
- [ITU-T Recommendation X.509] [3] (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 08/05.

**Co-operation and liaison**

- ISO/IEC/JTC1/SC7/WG7 (Software and Systems Life Cycle Processes)
- ISO/IEC/JTC 1/SC27/WG2 (Cryptography and Security Mechanisms)
- ISO/IEC/JTC 1/SC27/WG4 (Security Controls and Services)

**Preparatory work offered with target date(s)**

Members from SC22/WG23 intend to work jointly to develop and submit an initial working draft following approval of the NWI prior to a first meeting.

**Signature:**

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 requirements for cultural and linguistic adaptability? No

-If yes, please specify on a separate page

**Comments and recommendations of the JTC 1 or SC XXSecretariat** - 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 22/WG 23

**Voting on the proposal** - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

**Date of circulation:**  
YYYY-MM-DD

**Closing date for voting:**  
YYYY-MM-DD

**Signature of Secretary:**

**NEW WORK ITEM PROPOSAL -  
PROJECT ACCEPTANCE CRITERIA**

<b>Criterion</b>	<b>Validity</b>	<b>Explanation</b>
<b>A. Business Requirement</b>		
A.1 Market Requirement	Essential <input checked="" type="checkbox"/> Desirable <input type="checkbox"/> Supportive <input type="checkbox"/>	Verification of the source of software is an increasingly important problem.
A.2 Regulatory Context	Essential <input type="checkbox"/> Desirable <input checked="" type="checkbox"/> Supportive <input type="checkbox"/> Not Relevant <input type="checkbox"/>	Application of the standard will likely be cited in warranties of fitness for particular purposes.
<b>B. Related Work</b>		
B.1 Completion/Maintenance of current standards	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
B.2 Commitment to other organisation	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
B.3 Other Source of standards	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
<b>C. Technical Status</b>		
C.1 Mature Technology	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
C.2 Prospective Technology	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
C.3 Models/Tools	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
<b>D. Conformity Assessment and Interoperability</b>		
D.1 Conformity Assessment	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
D.2 Interoperability	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
<b>E. Adaptability to Culture, Language, Human Functioning and Context of Use</b>		

<b>E.1 Cultural and Linguistic Adaptability</b>	Yes _____ No ___X___	
<b>E.2 Adaptability to Human Functioning and Context of Use</b>	Yes _____ No ___X___	
<b>F. Other Justification</b>		

## **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 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** Any other aspects of background information justifying this NP shall be indicated here.

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.