ISO/IEC JTC 1/SC 22/WG 23 N 0273

Proposed draft NWIP for software security APIs

Date	2010-08-31
Contributed by	Larry Wagoner
Original file name	NWIP ssapi 082510.doc
Notes	

New Work Item Proposal

February 2004

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2010-08-24	Proposer: SC22 WG23
Secretariat: National Body	**ISO/IEC JTC 1 N** XXXX 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.

Title (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 -- Security and Safety Applications Programming Interface (SSAPI)
Scope (and field of application) This new work item encompasses a common set of security controls within software.
Purpose and justification - attach a separate page as annex, if necessary Most vulnerabilities in software stem from a control that is missing, poorly implemented, or incorrectly placed in the code. This is not surprising since knowing which controls are needed and implementing a control correctly can require very advanced knowledge and exacting skill. For example, input validation, access control, authentication, and logging of incidents can be difficult to implement robustly. As many programmers routinely work in a variety of languages, having a common or very similar set of APIs for controls can reduce the likelihood of an incorrectly implemented control. The lack of properly implemented controls can have serious consequences for systems that are intended to implement confidentiality, integrity, or availability properties such as safety, security or privacy. This project will identify the needed controls, define their operation, and define their respective APIs. The behavior of each of these APIs will be fully specified. The developed set of standards will provide a centrally organized, high quality, and vetted definition for the most commonly needed control APIs. SSAPI will ultimately provide the needed basis for a widely used infrastructure across many programming languages that will improve the safety, security, robustness, uniformity, and testability of software.

Programme of work

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

__X__ 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?

__X__a. Default Timeframe

____b. Accelerated Timeframe

____c. Extended Timeframe

Relevant documents to be considered

- Open Web Application Security Project (OWASP) Enterprise Security Applications Programming Interface (ESAPI)
- 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 crypto standards of ISO/IEC JTC1/SC27

Co-operation and liaison

• 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

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		
Criterion	**Validity**	**Explanation**
A. Business Requirement		
A.1 Market Requirement	Essential _X__ Desirable ___ Supportive ___	Verification of the security and safety of software is an increasingly important problem.
A.2 Regulatory Context	Essential ___ Desirable _X__ Supportive ___ Not Relevant ___	Application of the standard will likely be cited in warranties of fitness for particular purposes.
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No_X__	
B.2 Commitment to other organisation	Yes ___ No_X__	
B.3 Other Source of standards	Yes ___ No_X__	
C. Technical Status		
C.1 Mature Technology	Yes ___ No_X__	
C.2 Prospective Technology	Yes _X__ No___	
C.3 Models/Tools	Yes ___ No_X__	
D. Conformity Assessment and Interoperability		

D.1 Conformity Assessment	Yes ___ No__X_	
D.2 Interoperability	Yes ___ No_X__	
E. Adaptability to Culture, Language, Human Functioning and Context of Use		
E.1 Cultural and Linguistic Adaptability	**Yes**_____ **No**___**X**____	
E.2 Adaptability to Human Functioning and Context of Use	**Yes**_____ **No**___**X**____	
F. Other Justification		

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 se, 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.