Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14228
Date:	2010-02-01
Replaces:	
Document Type:	Summary of Voting/Table of Replies
Document Title:	Summary of Voting on 6N14123, Text for NP ballot, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks – Specific requirements - Part XX: Alternative security mechanism for use with ISO/IEC 8802-11
Document Source:	SC 6 Secretariat
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	13

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

Result of voting

Ballot Information:	
Ballot reference:	Text for NP ballot, 6N14123
Ballot type:	NWIP
Ballot title:	Text for NP ballot, Information technology ?Telecommunications and information exchange between systems ? Local and metropolitan area networks ? Specific requirements ? Part XX: Alternative security mechanism for use with ISO/IEC 8802-11
Opening date:	2009-10-29
Closing date:	2010-01-29
Note:	

Member responses:	
Votes cast (18)	Belgium (NBN) Canada (SCC) China (SAC) Czech Republic (UNMZ) France (AFNOR) Germany (DIN) Greece (ELOT) Japan (JISC) Kazakhstan (KAZMEMST) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Netherlands (NEN) Russian Federation (GOST R) Spain (AENOR) Switzerland (SNV) United Kingdom (BSI) USA (ANSI)
Comments submitted (1)	Ukraine (DSSU)
Votes not cast (0)	

Questions:	
Q.1	"Do you accept the proposal in the attached NWI Proposal document as a sufficient definition of the new work item?"
Q.2	"Do you support the addition of the new work item to the programme of work of the joint technical committee?"

Q.3	"Do you commit yourself to participate in the development of this new work item?"
Q.4	"Are you able to offer a project editor who will dedicate his/her efforts to the advancement and maintenance of this project?"
Q.5	"Do you have a major contribution or a reference document ready for submittal?"
Q.6	"Will you have such a contribution in ninety days?"
Q.7	"Which standard development track is proposed?"

Answers to Q.1: "Do you accept the proposal in the attached NWI Proposal document as a sufficient definition of the new work item?"		
11 x	**Yes**	**China (SAC)** **Czech Republic (UNMZ)** **Greece (ELOT)** **Japan (JISC)** **Kazakhstan (KAZMEMST)** **Kenya (KEBS)** **Korea, Republic of (KATS)** **Luxembourg (ILNAS)** **Netherlands (NEN)** **Spain (AENOR)** **Switzerland (SNV)**
2 x	**No**	**United Kingdom (BSI)** **USA (ANSI)**
5 x	**Abstain**	**Belgium (NBN)** **Canada (SCC)** **France (AFNOR)** **Germany (DIN)** **Russian Federation (GOST R)**

Answers to Q.2: "Do you support the addition of the new work item to the programme of work of the joint technical committee?"		
10 x	**Yes**	**China (SAC)** **Czech Republic (UNMZ)** **Japan (JISC)** **Kazakhstan (KAZMEMST)** **Kenya (KEBS)** **Korea, Republic of (KATS)** **Luxembourg (ILNAS)** **Netherlands (NEN)** **Spain (AENOR)** **Switzerland (SNV)**
2 x	**No**	**United Kingdom (BSI)** **USA (ANSI)**
6 x	**Abstain**	**Belgium (NBN)** **Canada (SCC)** **France (AFNOR)**

		Germany (DIN) Greece (ELOT) Russian Federation (GOST R)

Answers to Q.3: "Do you commit yourself to participate in the development of this new work item?"		
5 x	Yes	China (SAC) Czech Republic (UNMZ) Kenya (KEBS) Korea, Republic of (KATS) Switzerland (SNV)
8 x	No	Greece (ELOT) Japan (JISC) Luxembourg (ILNAS) Netherlands (NEN) Russian Federation (GOST R) Spain (AENOR) United Kingdom (BSI) USA (ANSI)
5 x	Abstain	Belgium (NBN) Canada (SCC) France (AFNOR) Germany (DIN) Kazakhstan (KAZMEMST)

Answers to Q.4: "Are you able to offer a project editor who will dedicate his/her efforts to the advancement and maintenance of this project?"		
1 x	Yes	China (SAC)
11 x	No	Czech Republic (UNMZ) Greece (ELOT) Japan (JISC) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Netherlands (NEN) Russian Federation (GOST R) Spain (AENOR) United Kingdom (BSI) USA (ANSI)
6 x	Abstain	Belgium (NBN) Canada (SCC) France (AFNOR) Germany (DIN) Kazakhstan (KAZMEMST) Switzerland (SNV)

Answers to Q.5: "Do you have a major contribution or a reference document ready for submittal?"

2 x	**Yes**	**China (SAC)** **Kenya (KEBS)**
11 x	**No**	**Czech Republic (UNMZ)** **Greece (ELOT)** **Japan (JISC)** **Kazakhstan (KAZMEMST)** **Korea, Republic of (KATS)** **Luxembourg (ILNAS)** **Netherlands (NEN)** **Russian Federation (GOST R)** **Spain (AENOR)** **United Kingdom (BSI)** **USA (ANSI)**
5 x	**Abstain**	**Belgium (NBN)** **Canada (SCC)** **France (AFNOR)** **Germany (DIN)** **Switzerland (SNV)**

Answers to Q.6: "Will you have such a contribution in ninety days?"		
2 x	**Yes**	**China (SAC)** **Kenya (KEBS)**
8 x	**No**	**Czech Republic (UNMZ)** **Greece (ELOT)** **Japan (JISC)** **Korea, Republic of (KATS)** **Netherlands (NEN)** **Spain (AENOR)** **United Kingdom (BSI)** **USA (ANSI)**
8 x	**Abstain**	**Belgium (NBN)** **Canada (SCC)** **France (AFNOR)** **Germany (DIN)** **Kazakhstan (KAZMEMST)** **Luxembourg (ILNAS)** **Russian Federation (GOST R)** **Switzerland (SNV)**

Answers to Q.7: "Which standard development track is proposed?"		
16 x	**Default Timeframe**	**Belgium (NBN)** **Canada (SCC)** **China (SAC)** **Czech Republic (UNMZ)** **France (AFNOR)** **Germany (DIN)** **Japan (JISC)** **Kenya (KEBS)** **Korea, Republic of (KATS)**

		Luxembourg (ILNAS) **Netherlands (NEN)** **Russian Federation (GOST R)** **Spain (AENOR)** **Switzerland (SNV)** **United Kingdom (BSI)** **USA (ANSI)**
1 x	**Accelerated Timeframe**	**Kazakhstan (KAZMEMST)**
1 x	**Extended Timeframe**	**Greece (ELOT)**

Comments from Voters		
Member:	Comment:	Date:
China (SAC)	***Comment***	2010-01-27 11:10:39
Dr. Huang Zhenhai EMAIL: zhenhai.huang@iwncomm.com		
Korea, Republic of (KATS)	***Comment***	2010-02-01 08:29:26
We will nomiate expert later.		
Korea, Republic of (KATS)	***Comment File***	2010-02-01 08:29:26
CommentFiles/Text_for_NP_ballot,_6N14123_KATS.doc		
Switzerland (SNV)	***Comment***	2010-01-06 11:30:50
Hans-Rudolf Thomann		
United Kingdom (BSI)	***Comment***	2010-01-20 16:20:45
See posted comments		
United Kingdom (BSI)	***Comment File***	2010-01-20 16:20:45
CommentFiles/Text_for_NP_ballot,_6N14123_BSI.doc		
USA (ANSI)	***Comment***	2010-01-25 15:44:13
see attachment		
USA (ANSI)	***Comment File***	2010-01-25

		15:44:13
CommentFiles/Text_for_NP_ballot,_6N14123_ANSI.doc		

Comments from Commenters		
Member:	Comment:	Date:
Ukraine (DSSU)	***Comment***	2010-01-22 12:52:09
abstain		

Template for comments and secretariat observations

Date: 29 January, 2009	Document: **6N 14123**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
KR	1. Scope	1st Para.	ed	Duplicate “for”	Delete one “for”	
KR	8.1.4.10.1, 8.1.4.10.2, 8.1.4.10.3, 8.1.4.10.4	Figure 44, 45, 46, 47	te	There are KD_HMAC_SHA-256 functions in these Figures. However, there is no description about this function.	It is necessary to add detailed descriptions of this function or refer to suitable reference.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Title: **Comments accompanying the UK vote of disapprove on 6N14123, NP ballot - ISO/IEC 8802-xx-Alternative security mechanism**
Date: **15 January 2010**
Source: **UK**

Setting aside the technical aspects of the proposal found in 6N14123 the UK is concerned that the text is presented as an Annex to {ISO/IEC8802-11 | IEEE 802.11}.

It is clear that the base IEEE 802.11 standard will develop within IEEE 802 and that the ISO/IEC equivalent text will not necessarily remain aligned.

And indeed given the existence of the PSDO Agreement, the IEEE 802 may not wish to maintain this two-track approach and might in the future request that ISO/IEC withdraw the base standard.

In either case the problem is that this security amendment would no longer be coordinated with the base standard to which international vendors will produce products. And of course if the base standard were withdrawn, the Annex would have no natural home.

From reading the SC6 Tokyo Resolution (6.1.4) it seems that the key words are “for adoption as a stand-alone standard”. This means that there is no reliance upon the ISO/IEC 8802-11 base standard and that this proposal should stand independently from the IEEE 802 work. If this were the case then ISO/IEC (through its Project Editor) would have ownership of the entire area under consideration.

The UK believes that this approach would be the best way forward although it is appreciated that this would result in considerably more work for China. But if this were to be the submission then all the issues associated with interactions etc between ISO/IEC and the IEEE 802 would, for this topic, be resolved such that attention and focus could be directed to the technical aspects of the proposal.

The UK also objects to the proposed amendment being numbered in the ISO/IEC 8802-xx range as this was clearly set aside for the family of standards coming out of the IEEE 802 to provide a very visible linkage that these pieces of work were actually one of the same thing. It is clear that the Chinese proposal falls outside this category.

On this basis the UK disapproves this NWI proposal.

NP Letter Ballot

VOTE ON A PROPOSED NEW WORK ITEM

ISO/IEC JTC 1/SC6 6N14123

Date of Circulation of NP: **2009-10-29**

Date of Ballot Close: **2010-01-29**

Please return all votes and comments directly to the JTC 1/ (SC 06) Secretariat by the due date indicated.

Proposal for a new work item on

Title: Text for NP ballot, Information technology—Telecommunications and Information exchange between systems – Local and metropolitan area networks –Specific Requirements—Part XX: Alternative security mechanism for use with ISO/IEC 8802-11

Any proposal to add a new item to the programme of work shall be voted on by correspondence, even if it has appeared in the agenda of a meeting.

A. Vote		**YES**	**NO**	**Comments**
Q.1	Do you accept the proposal in document JTC 1 (SC) N 6N14123 as a sufficient definition of the new work item? (If you have responded "NO" to the above question, you are required to comment.)	___ _	_X_ _	See Attachment
Q.2	Do you support the addition of the new work item to the programme of work of the joint technical committee?	___ _	_X_ _	____
B. Participation				
Q.3	Do you commit yourself to participate in the development of this new work item?	___ _	_X_ _	____
Q.4	Are you able to offer a project editor who will dedicate his/her efforts to the advancement and maintenance of this project? (If "YES," please identify .....)	___ _	_X_ _	____
C. Documentation				
Q.5	Do you have a major contribution or a reference document ready for submittal?	___ _	_X_ _	____
Q.6	Will you have such a contribution in ninety days?	___ _	_X_ _	____
Q.7	Which standard development track is proposed			_____

P-member Voting: National Body: United States	Date: __2009-11-17__	Submitted by: Name _____

Template for comments and secretariat observations

Date: 2009-11-17	Document:

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
US1	Purpose and Justification		ge	The proposal for the NP asserted that "current WLAN international standards contain serious security loopholes which need to be dealt with by enhanced security mechanisms". The justification is based on three issues that are based on either legacy or transitional security protocols of ISO/IEC 8802-11 and 8802-11 Amd6 (see introductory text of Clause 8.3.1 of Amd6), however there is nothing in the justification that suggests that the RSNA security protocol defined in ISO/IEC 8802-11 Amd6 Clause 8.3.3 (CCMP: CTR mode AES with CBC-MAC protocol) is not a sufficient security protocol for ISO/IEC 8802-11 networks. (Note: this security protocol is the basis for a security mechanism commonly known and certified as Wi-Fi Protected Setup 2 (WPA2).	If the NP justification is based on "serious security loopholes in WLAN international standards", please identify these issues in relation to the security protocol defined in ISO/IEC 8802-11 Amd6 Clause 8.3.3.	
US2	Purpose and Justification		ge	There is no justification given as to why the RSNA security protocol defined in ISO/IEC 8802-11 Amd6 Clause 8.3.3 is not a sufficient security protocol; therefore the NP proposal MUST contain a compelling justification why there should be a new ISO standard that duplicates the capabilities in an already approved ISO standard.	Provide an updated justification that provides a compelling justification why this duplicate security protocol is needed. The explanation needs to justify the duplication, which is contrary to good practice as articulated in the *JTC1 Directives* (clause 6.2.1.3) and the WTO's *Agreement on the Technical Barriers to Trade.*	
US3	Purpose and Justification		ge	The NP proposes the definition of an alternate security mechanism for ISO/IEC 8802-11 that does not integrate into the capabilities discovery and interface management mechanisms defined in ISO/IEC 8802-11 and amendments to this interface standard that either have already been defined, or are currently being defined, by the IEEE 802.11 Working Group. These extensions to the ISO/IEC 8802-11 standard include technologies in the area of the secure protection of interface management frames, fast roaming of STAs from AP to AP, higher throughput extensions to PHY layer etc. (IEEE approved amendments to ISO/IEC 8802.11 that aren't supportable by the NP include: IEEE 802.11e/j/k/n/r/ and w. Current Work In Progress amendments include: IEEE 802.11 p/s/u/v/z/aa/ac/ad).	Provide a compelling justification for an NP that will result in an ISO/IEC 8802-11 feature isolated from all amendments to the IEEE 802.11 standard since 2003 and any future amendments.	
US4	Market			The NP states that the market requirement is "essential,"	Provide further details on the nature of the market	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
	Requirement			however there appears to be no market demand for WAPI outside China. Over a billion devices that incorporate the security protocol defined in ISO/IEC 8802-11 Amd6 are being used successfully (with appropriate EAP methods) in consumer, enterprise, service provider and government segments around the world, including China. The demand in China appears to be the result of a regulatory requirement.	demand in China and the rest of the world and why an NP should be started for a technology that does not appear to have an international scope.	
US5	Regulatory Context			The NP proposal form states that the regulatory context is "essential," however, no explanation is provided. The only regulatory demand for the subject of the NP proposal is that of the regulatory body in China and is not a requirement of any other regulatory domain.	Provide further explanation and justification on why the regulatory context of this NP proposal is in fact "essential". Include reference to any relevant regulations in all countries in which there is a regulatory requirement for WAPI.	
US6	Cooperation & Liaison		ge	The documentation provided with the NP proposal (WAPI Draft) uses a variety of IE and error codes. Without coordination, it is likely these IE and error codes will cause interoperability issues between WAPI systems and ISO/IEC 8802-11 systems. The conflicts are likely with: IEEE approved amendments to ISO/IEC 8802-11 that include: IEEE 802.11e/j/k/n/r/w, current Work In Progress amendments that include: IEEE 802.11 p/s/u/v/z/aa/ac/ad. Such issues can only be avoided by cooperation and liaison with the IEEE 802.11 Working Group.	Add a MANDATORY requirement in the NP that states that this project, if approved, will work in cooperation with IEEE 802.11 to resolve these conflicts with current an future amendments to ISO/IEC 8802-11 made by the IEEE 802.11 Working Group.	
US7	Mature Technology		ge	It is asserted in the NP proposal that the technology used in the WAPI Draft is a mature technology. However, no justification is provided.	A justification should be provided that includes at least: • A description of any security reviews of WAPI (including the SMS4 cipher) by internationally recognized experts from multiple countries • A quantification of deployed systems and devices actually using WAPI today (not just implementing WAPI), with an explicit list of the names of operators running the largest systems and the size of those systems • An explanation of how WAPI can be included in a complete large system, in a manner that allows scalable provisioning of certificates in a secure	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of comment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
					manner, while maintaining the secrecy of private credentials • A description of how WAPI can be used in controller based architectures, such as those defined by IETF CAPWAP • A description of how WAPI secures management frames, in addition to data frames (features provided by IEEE 802.11w) • A description of how WAPI implements fast secure roaming (like that provided by IEEE 802.11r) • A description of how WAPI integrates with IEEE 802.11n (approved by the IEEE in September, 2009)	
US8	General Comments		ge	Clause 6.2.3 of the JTC1 Directives describes work that should be completed before submitting a proposal for a NP to an SC. The NP proposal does not include a "detailed plan of work covering the timetable, resource requirements and resource availability (technical and administrative)."	This NP proposal needs a detailed plan of work, including a plan for the incorporation of other amendments from the ISO/IEC 8802-11 standard series into the “WAPI-based” ISO/IEC standard series.	
US9	General Comments		ge	The US NB acknowledges that security mechanisms defined outside ISO/IEC 8802-11 Amd6 may be desirable in future revisions to ISO/IEC 8802-11 as security technologies advance and additional applications of the wireless technology are developed. The US NB would fully support these efforts in the appropriate technology forum.	The US NB believes the appropriate technology forum is the IEEE 802.11 working group because of their expertise in developing and extending the IEEE 802.11 standard over 19 years and because it is impractical for two independent forums to successfully modify the ISO/IEC 8802-11 standard in parallel. The US NB suggests that the WAPI technology be submitted to the IEEE 802.11 Working Group for consideration.	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.