China's Response to Contradiction Comments on 1N7904

Chinese National Body (SAC)

November 30, 2005

The following is a correspondence from the Chinese national body directly to all national bodies in ISO/IEC JTC1 to explain the issues and comments contained in JTC1 document entitled "Compilation of National Body Comments on JTC 1 N 7904, 30 Day Review for Fast Track Ballot ISO/IEC DIS 8802-11/Amd.7, Information technology - Telecommunications and information exchange between systems- Local and metropolitan area networks – Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - AMENDMENT 7: Specifications for Enhanced Security – WLAN Authentication and Privacy Infrastructure (WAPI)".

This document is also delivered to ISO/IEC central secretariat, JTC1 secretariat and other related parties for their reference. It is understood that because the proposal covered in this correspondence has entered ballot stage, no official discussions are allowed. This document is a direct correspondence between Chinese national body and related parties.

1. Comments Need Immediate Attention

As per the resolution of ISO/IEC SWG meeting on May 17, 2005 in ISO headquarters, Geneva, Chinese National Body resubmitted WAPI proposal to ITTF for fast track ballot starting on Sept. 7, 2005. On Sept. 6, 2005, ISO Secretary General Alan Bryden and IEC General Secretary Aharon Amit issued a decision to start fast track process for both IEEE 802.11i and WAPI proposal and directed that regardless of what happens in the one month review period, both proposals will starting the 5 month ballot on October 7 simultaneously and end at the same date. WAPI proposal was given a new number 1N7904 and on October 7, it entered 40.20 ballot stage along with U.K. NB's 11i (now 1N7903). However, Chinese National Body noticed that prior to entering the ballot stage, 11 national bodies have made contradiction comments and observations on 1N7904.

Chinese national body has always welcomed comments and we have made great efforts to accommodate comments and address any concerns raised about WAPI during the past year. Although WAPI has entered "no comment" period, and the comments can be resolved during the ballot resolution process, we believe that they cannot be ignored at this stage and explanations cannot be delayed. We have noticed that some NBs have stated that if the issues they raised were not resolved they would vote negatively on WAPI.

Therefore, Chinese National Body has to respond to those comments. However, we are in an awkward situation that both proposals have entered “no comment” period and no scheduled technical meetings will take place before the end of ballot. The only available means for China is to make direct contact and communicate actively and positively with national bodies which provided comments. But this would then leave out those NB’s who have seen those comments but may not see Chinese NB’s explanations. This would limit the effectiveness of our explanation and may weaken the support for WAPI.

Therefore, a general summary of comments and explanations is necessary and should be sent to all national bodies within JTC1 and SC6.

2. Summary of Comments

The comments can be summarized into 10 issues:

Issue 1: 1N7904 (WAPI) has contradictions with other standards. The contradictions should be resolved by ITTF and JTC 1 Secretariat in accordance with JTC 1 Procedures clause 13.2 before ballot voting commences.

Issue 2: 1N7904 (WAPI) is not a fast-track proposal for a draft standard but for a draft amendment to an existing standard. Therefore, the note from ITTF on page III is rather confusing.

Issue 3: The JTC 1 Directives state that the fast-track process

applies only to existing standards (from any source) that are submitted without modification. The text in 1N7904 shows significant changes from the Chinese Standard GB15629.11 of 2003 and from the Chinese contribution in SC6 N12687. It is not eligible for fast track processing.

Issue 4: 1N7904 (WAPI) Clause 8.1.3 contradicts ISO/IEC IS 9594-8:2001. It defines a new digital certificate format in clause 8.1.3. However, given ISO/IEC IS 9594 governs certificate formats, this topic is out of scope for an amendment to ISO/IEC IS 8802-11. 1 N 7904 does not justify its deviation from ISO/IEC IS 9594.

Issue 5: 1N7904 (WAPI) Clause 8.1.4.2 is outside the scope of ISO/IEC IS 8802-11:2005. It defines a new authentication scheme in clause 8.1.4.2. However, authentication schemes are outside the scope of an amendment to ISO/IEC 8802-11.

Issue 6: 1N7904 (WAPI) Clause 8 contradicts clause 8.2 of ISO/IEC IS 8802-11:2005. It deletes the definition of WEP. Adoption of 1 N 7904 would instantly render every existing WEP-only device non-conformant, which is undesirable for an international standard.

Issue 7: 1N7904 (WAPI) was developed using a process contradicting ISO/IEC TR 8802-1:2001. ISO/IEC TR 8802-11:2001 specifies a process for collaboration between JTC1/SC6/WG1 and IEEE 802 that is designed to ensure “rigorous technical appraisal” by

all stakeholders, including ISO/IEC NBs and IEEE 802.

Issue 8: 1N7904 (WAPI) specifies a new encryption method without providing any details about design or robustness. This has proven to be a very bad approach for LANs, and does not give an impression of high reliability.

Issue 9: If WAPI achieves the status of ISO standard, China could decide to close their borders to non-WAPI compliant wireless LAN products whereas Chinese manufacturers would not be faced with such constraints in their exports from China.

Issue 10: The WAPI proponents in China have been able to carry the day in the Chinese National Body but there is evidence that this group does not have the full backing of the Chinese leadership at the ministerial level. Therefore not supporting the WAPI standard will not necessarily hurt the relationship with China.

3. National Bodies and Issues

NB / Issue No.	USA	UK	France	Germany	Japan	Nether-land	Italy	Switz-land	Sweden	New-zealand	Aus-tralia
Issue1		●	●	●		●	●	●	●		
Issue2								●			

Issue3		●									
Issue4	●					●				●	●
Issue5	●		●	●	●	●	●	●	●	●	●
Issue6	●			●		●		●		●	●
Issue7	●	●	●	●	●	●	●	●		●	●
Issue8					●			●			
Issue9						●					
Issue10						●					

4. General Impressions

Chinese National Body has carefully reviewed these comments and found that most of the issues have been raised in many related international meetings held previously on this subject and have been explained and addressed by the Chinese national body with great detail in documents presented to those meetings. Only issue 2 and issue 10 are newer issues. Issue 2 is a minor point about the inaccurate wording of ITTF's notice. Issue 10 actually is not a proper topic and should not be a factor for consideration.

Nevertheless, in order to remove any remaining concerns and to demonstrate the qualities and strengths of WAPI for ISO/IEC standard, we will answer again those questions in detail in this document. We hope

that our explanations will be satisfactory to national bodies and win their support for WAPI.

5. Addressing the Specific Concerns

Issue 1: Contradiction

Some comments state: *"The ISO/IEC JTC1 Directives requires that voting members must review and comment on documents and that any contradictions with other ISO or IEC standards must be resolved before ballot voting. WAPI has multiple known "contradictions" with other standards. The contradictions should be resolved by ITTF and JTC 1 Secretariat in accordance with JTC 1 Procedures clause 13.2 before ballot voting commences."*

Response from China:

The following aspects should be taken into consideration:

1) A concern has already been addressed.

This issue was raised during the France meeting (August 29-Sept. 2, St. Paul De Vance, SC6 2005 plenary meeting) and Chinese national body has provided detailed response to it in SC6 France meeting.[1]

[1] See Attachment#4 "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003 -WAPI Status" and Attachment#5 6N12960 "Notes from Chinese national body" (August 31, 2005).

2) WAPI has gone through extended reviews.

From August 2, 2004 to Sept. 6, 2005, WAPI has gone through an extremely long and extended review period. This period far exceeds the one month review for fast track procedure and the 2-3 month review for NP procedure.

3) National bodies had numerous opportunities and long period to study the proposal and make comments.

During this period:

- August 2, 2004, WAPI was circulated on to national body for three month review. (1N7506)
- WAPI had received comments on August 25 and 26, 2004. (6N12712 and 6N12713)
- In July 2005, WAPI proposal was distributed for comments by ISO/IEC Central Secretariat and posted on ISO/IEC websites for public access and review. (WAPI N 16)
- In August 2005, WAPI was resubmitted to ITTF for fast track ballot.

4) Comments were addressed in five international meetings

During the one year review period, many comments were received and careful attention was given to them.

Comments on WAPI were addressed fully in the following meetings:

- Nov. 8-12, Orlando (U.S.) SC6 2004 plenary meeting

- Feb. 21-23, Frankfurt (Germany) SC6/WG1 special meeting
- May 17, ISO/IEC special work group meeting in Geneva (Switzerland)
- August 8-12, ISO/IEC Beijing (China) Special Working Group meeting
- August 31-Sept. 2, SC6 St. Paul De Vance (France) 2005 plenary meeting

5) Results of these meetings

- In Orlando meeting (Nov. 8-12, SC6 2004 plenary meeting), WAPI's qualification for fast track procedure was discussed and a positive answer was made.
- In Orlando meeting, IEEE announced that "*WAPI and 11i are not mutually exclusive. They can both reside within ISO/IEC 8802-11 and invoked when needed.*"[2]
- In Orlando meeting, a resolution was adopted allowing WAPI and 11i "*be progressed independently and concurrently within SC6.*"[3]
- In Jan. 2005, JTC1 Secretariat ruled that WAPI has fulfilled the one month review period and can enter ballot stage.[4]

---

[2] Comments from IEEE delegation, 6N12768 (Attachment#6)

[3] Orlando, SC6 2004 plenary meeting, 6N12765 (Attachment#7)

[4] Letter from Lisa Rajchel, Secretariat, ISO/IEC JTC 1,Jan 28,2005:"*As the proposal from China is for an amendment to ISO/IEC 8802-11, it technically should be approved for Fast Tack processing by ISO/IEC JTC*

- In Geneva meeting (May 17,2005, ISO/IEC special work group meeting), the final resolution, reached through the principle of unanimous consensus, authorized the start of WAPI ballot on September 6, 2005. The resolution was agreed to by US, UK, and IEEE representatives. [5]

1/SC 6 prior to its submission to the ITTF. However, I note that documentation from the ISO/IEC JTC 1/SC 6 Orlando meeting indicates that processing your proposal as a potential Fast Track document was extensively discussed by ISO/IEC JTC 1/SC 6 participants as an option. Therefore, I would rule that your proposal can go forward without additional approval from ISO/IEC JTC 1/SC 6."

"Further, clause 13 of the ISO/IEC JTC 1 Directives also states that all documents for Fast Track processing should first be sent to JTC 1 National Bodies for a 30 day Fast Track review to determine if there are any contradictions to other JTC 1, ISO, or IEC standards. This would then be followed by a five month formal letter ballot. However, given the extensive discussions that have already taken place within ISO/IEC JTC 1/SC 6 with respect to the Chinese proposal, I believe that the 30 review period has been fulfilled and that the document can immediately be issued for the five month ballot." – quotes from the letter from Lisa Rajchel, Secretariat, ISO/IEC JTC 1 to China NB, Jan. 28, 2005.

[5] The Geneva resolution (Attachment#8) was reached with a principle of unanimous consensus agreed by all related parties in the meeting. To change the resolution should also require unanimous consensus by all parties. China notices that some parties have reversed their positions in the France SC6 plenary meeting. This is a deviation from JTC1 directives. JTC1 directive states: "*12.2.6 Both NBs and any representatives presenting views at previous levels shall attempt to avoid confusion and delay that could result from different positions being declared (see 2.6.1.3) at different levels."*

- In Beijing meeting (August 8-12,2005), Chinese national body announced that the two proposals are not mutually exclusive and both can reside as alternative solutions within ISO/IEC 8802-11 and invoked when and where needed. This principle was firmly established in Beijing meeting.
- In Sept. 2005, a decision was made by ISO/IEC central secretariat that WAPI will enter ballot with 11i on October 7, 2005. This is a sound and wise decision.

6) China obeyed the rules

There is an argument that Chinese National Body disrespects the rules and normal procedures by pushing WAPI into ballot. We strongly deny this groundless and unfair criticism.

Chinese national body has carefully studied the rules and procedures and strictly complied with them. Nothing has been done by China that violated any rules and principles.

We have to point out that it was a series of unfair treatments and rule violations by other parties that prompted the special Geneva meeting. In that meeting, after hearing all facts and arguments, a unanimous decision was made to continue the suspension of 11i ballot and through unanimous consensus to start fast track ballot for both WAPI and 11i on September 7. Any change to that resolution has to be agreed to by all parties involved in that meeting.

Conclusion:

WAPI's contradiction with 11i proposal was identified during the comment period in August 2004 and has been fully discussed in a series of meetings including SC6 2004 plenary meeting in Orlando, the Geneva SWG meeting, Beijing meeting and SC6 2005 plenary meeting in France (St. Paul De Vance). The contradiction has been resolved and a series of decisions have authorized WAPI to enter ballot stage. These decisions reflect a determination that the perceived "contradiction" should prevent neither WAPI nor 11i from entering ballot on October 7 and the contradiction should not be used as a ground to vote against WAPI. Entering of WAPI into the ballot stage on October is a legitimate, considerate and constructive decision.

Issue 2: An amendment, not a standard

The comment states: *"This is not a fast-track proposal for a draft standard but for a draft amendment to an existing standard. Therefore, the note from ITTF on page III is rather confusing."*

Response from China:

Both WAPI and 11i are proposed security enhancement mechanisms. They are amendments to ISO/IEC 8802-11 base standard. They can not

mutually not mutually exclusive and both can reside as alternative solutions within ISO/IEC 8802-11 and invoked when and where are needed.

Issue 3: WAPI not eligible for Fast Track because texts changed

The comment states:

"The JTC 1 Directives state that the fast-track process applies only to existing standards (from any source) that are submitted without modification. The text in J1N7904 shows significant changes from the Chinese Standard GB15629.11 of 2003 and from the Chinese contribution in SC6 N12687. Unless it can be demonstrated that the text of N 7904 was identical to the published Chinese Standard at the time of submission, it is not eligible for fast track processing."

Response from China:

1) This is an old issue.

This question was raised by IEEE delegation to the ISO/IEC Beijing meeting.

2) We have explained before.

Answer to this question was provided by the Chinese delegation in SC6 2005 France (August 31-Sept. 2, St. Paul De Vance) plenary meeting. In document entitled "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN -003-WAPI Status," (Attachment#4) Chinese national body provided the

following explanation:

"Why the Changes?

There is an opinion that WAPI proposal has changed several time and it shows that it is not mature.

Chinese NB wishes to call attention to the following facts:

- *WAPI is a mature technology and has been adopted as China's national standard.*
- *The changes were minor and were made mainly to make it more compliant with International Standardization requirements.*
- *WAPI's structural integrity and strength in security mechanism has not been weakened.*
- *Changes before fast track balloting is authorized by ISO/IEC directives.* [6]

3) Fast Track does not prevent comments and suggestions"

JTC1 Directive states:

"Prior to submission of a document for fast-track processing, a P-member or Category A liaison organisation of JTC 1 may request that the document be submitted through the JTC 1 Secretariat to one or more SCs for informal comment or discussion among the interested parties. Any comments on format, technical content, completeness, etc. could be

[6] See Attachment#4 "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status," presented by Chinese national body in France SC6 2005 plenary meeting.

considered by the requester prior to formal submission of the document for fast-track procedure. [7]*"*

4) Changes does not violate Fast track procedure

The procedure does prevent changes after introduction and before fast track ballot. Changes are prohibited only during the ballot process.

JTC1 Directives states:

"M.7.3.1.3 Changes during transposition

What are the expectations of the proposer toward technical and editorial changes to the specification during the transposition process?

It is at the discretion of the Recognised PAS Submitter to withdraw the document from the transposition process at any point prior to publication. It is also the right of the Recognised PAS Submitter to request that the document remain unchanged throughout the transposition process. Such a request should be clearly stated in the Explanatory Report, and may be an issue in the ballot process. Changes to the specification during the ballot process are, however, not acceptable as they will lead to confusion. [8]*"*

5) NP can be switched to fast track procedure

JTC1 Directive states:

"As described in 12.1 an SC may suspend normal processing in favour

---

[7] JTC1 Directives, 5th Edition, page 55.

[8] JTC1 Directives, 5th Edition, page 62.

of the fast-track procedure (to be initiated by a P-member or a Category A liaison organisation of JTC 1) provided that:

- *the SC agrees that the intended fast-track document is suitable to satisfy the requirements of the existing project; and*
- *the SC agrees to the use of the fast-track procedure and so notifies JTC 1.* [9]*"*

It is a fact that SC6, JTC1 and ISO/IEC Secretariats have all agreed to put WAPI into fast track process.

6) NBs may suggest changes in ballot

According to JTC1 directives regarding votes on fast track DISs: NBs may vote in the way of

"disapproval of the DIS (or DAM) for technical reasons to be stated, with proposals for changes that would make the document acceptable (acceptance of these proposals shall be referred to the NB concerned for confirmation that the vote can be changed to approval); [10]*"*

If the ballot may suggest changes, pre ballot changes to accommodate comments are also justified.

Conclusion:

WAPI is a mature technology. The change of texts of WAPI proposal does not impact its technical strength, structural integrity

[9] JTC1 Directives, 5th Edition, page 56.
[10] JTC1 Directives, 5th Edition, page 45.

or security performance. The changes are intended to make it fit for international standards and world-wide use. The changes are made by taking comments and suggestions during the comment period, and to help reach a consensus. Unless there is evident proof that WAPI has fatal security flaws and cannot deliver a trustable security solution, WAPI's fitness for international standard should not be questioned.

Issue 4: On WAPI Deviation from ISO/IEC IS 9594

The comment states:

JTC 1 N 7904 defines a new digital certificate format in clause 8.1.3. However, given ISO/IEC IS 9594 governs certificate formats, this topic is out of scope for an amendment to ISO/IEC IS 8802-11. JTC 1 N 7904 does not justify its deviation from ISO/IEC IS 9594.

Response from China:

In fact, 1N7904 (WAPI) defines two kinds of certificate formats. One of which is the X.509 v3 certificate format and it is mandatory. The other is GBW certificate format and it is optional.

Therefore, there is no contradiction between WAPI certificate format and other international standards. On the contrary, WAPI provides more options for WLAN certificate format.

Issue 5: Authentication outside the scope of 8802-11 (and of

SC6)

The comment states: "*1 N 7904 (WAPI) Clause 8.1.4.2 is outside the scope of ISO/IEC IS 8802-11:2005. It defines a new authentication scheme in clause 8.1.4.2. However, authentication schemes are outside the scope of an amendment to ISO/IEC 8802-11.*"

Response of China:

1) Again, this is not a new issue.

In Beijing and in France meetings, IEEE had made this argument. Chinese national body had presented a complete and convincing rebuttal during those meetings. [11]

2) WAI is needed for WLAN security

WAPI is an advanced and new security mechanism designed to address the defects and inadequacies of WEP in WLAN. WAPI exceeds with innovative technological concepts of peer access control and mutual authentication.

WAPI implements the security of MAC layer, and Certificate mechanism adopted in WAPI is just a means to implement the MAC layer security.

Furthermore, the state machine of WAPI is controlled by the MAC

---

[11] See Attachment#4 "SC6WG1-SPV016-Item 8.3.2-SC6WG1-CHN-003-WAPI Status", presented at SC6 France meeting.

protocol, and WAPI and MAC protocols have become an integrated part.

WAPI is an intact mechanism. WAPI's components form a complete and trustable solution to eliminate the existing security loopholes in WLAN systems.

3) 11i 4-way handshake protocol and 802.1x have similar situations

On the other hand, 4-way handshake protocol is defined in IEEE 802.11i, and the packets of 4-way handshake protocol are carried in the data frames of MAC layer. If WAPI goes beyond SC6 scope, then according to the same logic, the 4-way handshake protocol is not belonging to layer 1 and layer 2 specifications, and is not within the scope of SC6 WG1.

Additionally, IEEE 802.11i adopts IEEE 802.1x as authentication protocol of the security mechanism. Although IEEE 802.1x is not included in the text content of IEEE 802.11i, it should be regarded as one necessary part of IEEE 802.11i. The packets defined in IEEE 802.1x are also carried in the data frames of MAC layer. If WAPI goes beyond SC6 scope, then according to the same logic, IEEE 802.1x is beyond the SC6/WG1. Furthermore, IEEE 802.1x is just an internal standard of IEEE, not an international standard until now.

Why no one suggested IEEE to submit IEEE 802.1x to ISO/IEC for

ballot first, then adopt IEEE 802.1x in IEEE 802.11i? [12] Is this a display of double standard?

4) We believe that the physical layers should not be used to disintegrate WAPI

- The layers should not be a barrier to prevent technological development and the availability of urgently needed security solution.
- The standards should be evaluated based on its technical necessity and merits.
- Especially for WLAN, providing a secure solution should be the primary concern and motive.
- WAPI does not present a problem to other international standards.

Conclusion:

So, WAPI is designed specifically for WLAN to resolve security problem of WEP, and it should be within the scope of SC6 WG1. Furthermore, WAI is an integral part of WAPI, an innovative technology and so far the best known way to address the certification

---

[12] For more Chinese comments on 11i, please see Attachment#3 "Compilation of National Body Comments on JTC 1 N 7903, 30 Day Review for Fast Track Ballot ISO/IEC DIS 8802-11/Amd.6".

problems in WLAN systems.

The international community needs a timely and trusted security solution. We should not let minor and rigid interpretation of procedures to prevent the access of international community to an urgently needed technology.

Issue 6: Deleting the definition of WEP

The comments state: *"JTC 1 N 7904 clause 8 contradicts ISO/IEC 8802-11:2005 clause 8.2 by deleting the definition of WEP. Adoption of JTC 1 N 7904 would instantly render every existing WEP-only device non-conformant, which is undesirable for an international standard. It would also mean that these devices would become illegal in at least some jurisdictions, without any compensation to the owners of these devices."*

Response from China:

1) Again, this is an old issue. Chinese national body has explained the reason for not including WEP in the solution in documents presented in the Beijing and SC6 France meetings. [13] However, in order to allow more national bodies to understand China's

[13] See Attachment#4 "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status" and Beijing meeting document "WAPI-CHN-T106_Response to Comments on WAPI" available upon request from the Chinese national body.

considerations and intentions, we will make an explanation again in this document.

2) The fact that WAPI does not provide backward compatibility was a careful decision based on technical evaluation, security concern and the strong demand for uncompromised and reliable security mechanism by the international community.

3) It is a well known fact that WEP has serious security flaws, having been described as a “security disaster”. It should be eliminated as soon as possible. WAPI is designed to replace it to provide better security solution.

4) Chinese experts have pointed out that any attempt to force new security solutions to provide backward compatibility to WEP is good for business interests and investment protection, but bad for security because it would compromise the security solution, reduce the levels of protection, and leave users and networks vulnerable to various kinds of attacks. [14]

5) Any proposal which retains WEP in order to protect past investment would constitute a trade off between security and commercial interest and should not be encouraged or accepted. It is not a good practice nor is it in the best interests of world-wide

[14] See detailed analysis on “Attachment#9-SC6WG1-SPV017-Item 8.5-SC6 WG1-CHN-004-Detailed Comments on IEEE 80211i” presented at SC6 France plenary meeting on August 31-Setp.2, 2005.

consumers, WLAN international standardization or the international community.

6) International standard may become national and regional standard and therefore may be implemented in important national public facilities and infrastructures. The standard may be implemented in transportation, finance, communication, energy and other nationwide networks. Compromised security solutions may expose those networks to security risks and threaten national security.

7) When a better and more reliable security solution is available to protect the interests of consumers and communities, making this kind of trade off and compromising security is an irresponsible behavior. Future WLAN market will be hundreds times of current size, to focus on current market interests and at the same time put the huge future market under constant security risk is a shortsighted behavior. Therefore, providing the uncompromised, reliable, best possible security solution should be the utmost concern.

8) WAPI provides such a solution. It can reside with 11i as an alternative solution and satisfy those who do not want to contain WEP in their WLAN systems.

9) As to “compensation to the owners of these devices,” it should not

be a topic to discuss in this forum. It should not be a topic in the discussion of ISO/IEC standardization activities.

However, we believe that the responsibility should be on those who made, promoted and marketed flawed security solutions like WEP at the first place.

Conclusion:

WAPI does not provide backward compatibility to WEP and therefore maintains the highest level of security and is an alternative solution to those who want uncompromised and reliable solutions. The international community should see the benefits of this strategic decision and be aware of the security risks in those standards which still contains the WEP problem.

An international standard containing a security mechanism with known defects will not only hurt the prestige of ISO/IEC, but also may reduce it's chances of been adopted into national and regional standards.

Issue 7: WAPI did not follow SC6-IEEE Cooperation Process

The comments state: *"ISO/IEC TR 8802-11:2001 specifies a process for collaboration between JTC1/SC6/WG1 and IEEE 802 that is designed to ensure "rigorous technical appraisal" by all stakeholders, including ISO/IEC NBs and IEEE 802. However, JTC 1 N 7904 was developed*

independently and without any coordination with the community co-developing ISO/IEC IS 8802-11 and its amendments, thus avoiding the necessary "rigorous technical appraisal".

Response from China:

1) This is not a new issue.

This has been one of the focuses of the WAPI-11i controversy. Within the past year, this argument has been raised many times by IEEE and some national bodies.

2) This issue has been resolved.

Decisions that WAPI does not violate the SC6-IEEE cooperation agreement and that WAPI can proceed within ISO/IEC structure have been made repeatedly in WAPI related meetings.

3) It is really annoying to see that this issue is raised again during the ballot period despite previous discussions and long after the results have been determined.

It may be understandable that some national bodies, which did not participate in any of the related meetings, do not understand the situation. But, it is very disturbing that U.S. and U.K. national bodies, which have participated in those meetings (Orlando, Geneva and France meetings) and agreed to those decisions, would raise this issue again.

4) Chinese national body has pointed out repeatedly the following points:

- We respect IEEE and recognize its contribution to ISO/IEC international standardization.
- There are many Chinese experts participating in IEEE activities.
- We are not against SC6-IEEE agreement, but we are against over-stating and misinterpreting of the agreement and the repeated making of unreasonable demands based on it.
- IEEE has been invited to provide comments on WAPI;
- IEEE has provided comments to WAPI proposal (in Orlando, Frankfurt, Geneva, Beijing and France meetings).
- It is improper and infeasible for Chinese national body to participate in IEEE standard activities;
- SC6-IEEE agreement does not apply to the WAPI situation;
- IEEE does not have exclusive right nor monopoly to make WLAN standards in ISO/IEC;
- WAPI must proceed in ISO/IEC.

5) SC6 has decided to process WAPI in ISO/IEC in 2004

This decision was made in SC6 2004 plenary meeting in Orlando Nov. 2004, after Chinese national body questioned the suggestion of submitting WAPI to IEEE for processing. The SC6 document states:

"The Chinese NB are encouraged, considering the co-operative working arrangements established between ISO/IEC JTC1 SC6 and the IEEE 802, to submit their specific proposal to JTC1 SC6 for processing.

This will then ensure that the proposal is reviewed in the appropriate international forum and, if accepted, will be included as an amendment to the ISO/IEC 8802-11 work for use in the international community." [15]

This document was approved unanimously in SC6 Orlando meeting.

6) Geneva meeting rejected the IEEE demand

IEEE delegation to May 17 Geneva meeting made another request to submit WAPI to IEEE processing. Chinese delegation expressed concern and objection. The meeting parties (China NB, U.K. U.S. IEEE, and ISO/IEC Central Secretariat representatives) finally agreed to process WAPI within ISO/IEC structure. [16]

7) Beijing meeting did not allow IEEE to make similar demand

Despite that all above decisions, before the Beijing meeting, IEEE again made another similar demand for processing WAPI under IEEE structure.

However, ISO/IEC central secretariat officials held the view that the issue has been decided and no more discussion on the topic was allowed.

8) The France meeting decides to process WAPI under ISO/IEC

- The SC6 France meeting (August 31-Sept. 2, St. Paul De Vance, SC6 2005 plenary meeting) did not request WAPI to comply with

[15] Orlando, SC6 2004 plenary meeting, 6N12765 (Attachment#7)

[16] ISO/IEC Central Secretariats report on Geneva meeting minutes, May 17, 2005.

the SC6-IEEE agreement, but instead put it under ISO/IEC complete jurisdiction.

Conclusion:

WAPI did not violate SC6-IEEE agreement; the agreement did not apply to WAPI; WAPI did receive comments from IEEE which is a C-liaison organization; WAPI is a legitimate candidate for ISO/IEC processing.

Therefore, SC6-IEEE agreement should not be used as a ground to disqualify WAPI for ISO/IEC standardization.

Chinese national body wishes that this is final explanation on this issue. If the explanation is not accepted by any body, we do not rule out the possibility to ask ISO/IEC TMB/SMB to make a final ruling to settle the issue permanently. [17]

Issue 8: WAPI Cryptographic Algorism not open

The comment states:

"1 N 7904 (WAPI) specifies a new encryption method without providing any details about design or robustness. This has proven to be a very bad approach for LANs, and does not give an impression of high

[17] For more information on this issue, please refer to Beijing meeting document "CNB-responsetoIEEEopeningremarks.ppt" and a special report "CNB-Understanding SC6-IEEE Cooperation: A Brief Review of Recent Positions and Decisions" available upon request from the Chinese national body.

reliability."

Response from China:

1) Again, this is an old issue.

Chinese national body has provided detailed response to this question in previous meetings. In the Beijing meeting during August 8-12, 2005, Chinese NB presented a document entitled "WAPI and Cipher Issue", which examines ISO policies on standardization of cryptographic algorism. [18]

In SC6 2005 plenary meeting in France, August 31-Sept. 2, 2005, Chinese NB further explained the issue in document reviewing the status of the WAPI proposal.[19]

2) There is no international standard in cryptographic algorism.

3) ISO council has determined in 1985 that cryptographic algorism is too political and decided not to pursue international standardization of cryptographic algorisms.

4) 11i's designation of AES as mandatory algorism, thus making it a de facto international standard and imposing it on the international community, is questionable.

5) Cryptographic algorism has sensitive political and security implications. There are laws and regulations governing

[18] ISO/IEC Central Secretariats document WAPI N33 (Attachment#10).

[19] See "WAPI-CHN-T708-Encryption issue" and Attachment#4 "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status"

cryptographic algorism in many nations. International standards should not supersede those laws and regulations but instead should allow compliance with them.

6) 1N7904 (WAPI) only defines a security protocol and does not mandate any cryptographic algorism. The security protocols and cryptographic algorisms are independent from each other. 1N7904 (WAPI) lists SMS4 algorism as an optional reference. According to local regulatory requirements and needs, different algorisms such as AES, TWOFISH or SEED etc. can be selected or implemented. The listed optional algorism SMS4 is owned by Beijing Data Security Technology Co. Ltd. (BDST). For more information, please contact BDST at: chinabdst@126.com. Therefore, 1N7904 (WAPI) does not impose any algorism to any body.
7) WAPI has provided the necessary information regarding SMS4 as required by relevant ISO standardization rules (ISO 9160).
8) WAPI's treatment of cryptographic algorism does not violate any ISO /IEC standardization rules.
9) The request for more openness of SMS4 algorism is beyond the scope of ISO/IEC requirements and should not be used to reject WAPI proposal.

Issue 9) China could exclude non-WAPI compliant products

The comment states:

"If WAPI achieves the status of ISO standard, China could decide to close their borders to non-WAPI compliant wireless LAN products whereas Chinese manufacturers would not be faced with such constraints in their exports from China."

Response from China:

1) This is not a new comment. During the Beijing meeting of August 8-12, a similar argument was made. Chinese national body responded and the issue was settled.
2) This is a speculative presumption which should not be a proper topic to discuss.
3) There was speculation that WAPI was developed in China for the purpose of protecting domestic market. It is not true. WAPI's objective was to provide enhanced security protection to the wireless communication systems. ISO/IEC 8802-11 standard contains serious defects which expose end users as well as important national infrastructures such as communication, transportation and financial networks and the general public to various kinds of security risks. The defects caused widespread concerns among the public and the government whose duty is to protect national security. To eliminate the security loopholes in WLAN standards, China started developing WAPI technology and

introduced it as a mandatory standard in May 2003. Such a measure to protect national security interests does not violate WTO-TBT agreement.

4) We are in the process to make international standards, not to decide how the standards are adopted and implemented at national and regional levels.
5) International standard is a voluntary standard. Even if WAPI and any other proposals become international standard, it does not guarantee they will be adopted into national and regional standards. There are many factors such as national security, performance, regulations, environment, prevention of deceptions etc. to determine whether and how fast they will be implemented.
6) Whether WAPI or other standards will be adopted and implemented in China may depend on not only relevant bounding international rules, but also the needs and requirement of China.
7) Chinese National Body has pointed out that WAPI and 11i are not mutually exclusive, they can both reside within ISO/IEC 8802-11 as alternative solutions and invoked when needed. Local needs and requirements may determine how these solutions are implemented.
8) For the sake of security and of the well being of international community, a timely security solution with the most reliable

security functions should be made available as an option to satisfy urgently needs of the international community.

Issue 10) WAPI does not have full backing of Chinese leadership

The comment states:

"The WAPI proponents in China have been able to carry the day in the Chinese National Body but there is evidence that this group does not have the full backing of the Chinese leadership at ministerial level. Therefore not supporting the WAPI standard will not necessarily hurt the relationship with China."

Response from China:

Chinese national body is very surprised, perplexed and concerned to see this comment. We strongly question the source of this information and its truthfulness. Chinese national body represents China as a nation to ISO/IEC. All positions and views below are authorized by the Chinese government.

1) Chinese national body demands to see the so called "evidence."
2) China strongly disagrees with the views expressed in this comment.
3) WAPI is an advanced and mature technology. It has the full backing of not only the Chinese leadership at all levels, but also

the 1.3 billion Chinese people.

4) Chinese national body has made this statement in SC6 France meeting: "*WAPI is an advanced mature technology. International community is in urgent need for such a security technology. Chinese government and 1.3 billion Chinese people strongly support WAPI. WAPI is a contribution of China to the international community. Chinese NB regards WAPI as an alternative solution which can be adopted according to local needs and requirements. WAPI proposal has passed extensive review and has been modified to adopt comments and suggestions. China has adopted thousands ISO/IEC standards. WAPI should benefit from a reciprocal relationship between China and ISO/IEC. Chinese NB does not see any reason to prevent WAPI from becoming an IS. For all considerations, WAPI deserves to be adopted into ISO/IEC standards.*" [20]

Conclusion:

China's full backing for WAPI is clear and beyond any doubt.

6. Conclusion

China has good intentions and legitimate reasons to develop the WAPI technology, adopt it as a national standard, implement it to protect

[20] See Attachment#4 "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status". Chinese national body, August, 2005, presented to SC6 2005 plenary meeting.

China’s consumer privacy, community interests, public facilities and national security at any proper time, and submit it for international standardization as an alternative security solution in the interests of international community. China has done extensive and careful studies on relevant international norms and procedures including those of WTO and ISO/IEC, and is confident that none of these considerations and activities constitutes any violations. China produced WAPI not for creating a trade barrier or to protect domestic market, but for the sake of information security not only in China, but also in the whole international community.

Chinese government has an obligation to provide a secure environment for our nation. China cannot accept anything which would expose the important national infrastructures, public facilities and the 1.3 Chinese people to the unscrupulous hackers and evil intruders.

Chinese national body believes that previous efforts and information provided in this document have fully addressed the comments and resolved the issues.

At the current stage, Chinese national body welcome any one, who has unanswered questions and concerns, to contact Chinese National Body directly so that an effective channel of dialogue is established to have full understanding and complete and satisfactory solutions.

7. Additional Observations from China

Chinese national body also wishes to take this opportunity to register the following observations on the recent events related to WAPI and 11i..

1) WAPI had been under review and continuous discussion for over one year, and yet it was complained that national bodies were not be able to review the documents.
2) We understand that WAPI related meetings may be too technical and boring and over the course of one year there is a lack of interest and participation. Suddenly in a short period between Sept. 7 and Oct.7, there is an eagerness to provide comments. This is a strange phenomenon.
3) Abstained from SC6 plenary and WG meetings, and yet complain that their rights to participate were denied.
4) Questions are raised time and again despite that answers and explanations have been provided in previous documents and meetings.
5) Documents generated in previous meetings were not read or carefully studied, nor were they taken into consideration in provided comments.
6) Same positions were presented time and again despite that it has been rejected by previous formally adopted resolutions.
7) Reversal of positions at different levels.
8) Among the two proposals, criticism was given exclusively to one,

while paying no attention to the other.

9) In reviewing proposals dealing with the extremely important security issues, great attention was paid to none-essential issues and hear-sayings on one proposal, meanwhile totally neglect the necessary analysis for the other proposal. This is obviously unfair and inequitable.

10) Speculative presumptions are used to criticize a proposal.

11) Hear-sayings are presented as evidence to influence balloting process.

12) Resolutions, based on due process and unanimous consensus, are violated.

These phenomena can hardly be regarded as been open, fair, impartial, responsible, or justified.

ISO/IEC has established great reputation and prestige by upholding the principles of openness, fairness, responsible, and due process. Chinese national body has made every effort to help maintain this tradition. But above actions and behavior deviates from it. China will continue to observe the related development and may consider necessary actions to deal with it at a proper time.

8. Final Conclusion

After more than a year of rigorous reviews, comments, discussions

and presentations, after accommodating some comments and after convincingly answering and detailed explaining remaining questions and concerns, it is evidently clear that WAPI is a mature, advanced, reliable and qualified alternative security solution for ISO/IEC 8802-11 WLAN standards. It satisfies all the requirements for international standardization. It has the full support from the Chinese government and the 1.3 billion Chinese people. China calls all fellow national bodies to approve WAPI to make it an alternative security solution to help protect the information security of the whole international community.