A report to ISO/IEC Central Secretariats and TMB/SMB

With copies to JTC1 and SC6 Secretariats

Analysis and Rejection of WAPI Ballot Comments:

A Supplement to China's appeal document Unjust Activity, Undue Process, Unfair Results: Ethical and Procedural Violations in WAPI-11i Fast-track Process submitted on April 29, 2006 to ISO/TMB IEC/SMB

With Attachment:

China's Response to Contradiction Comments on 1N7904

（Chinese National Body, Nov. 30, 2005）

Submitted by

Chinese National Body (SAC)

May 15，2006

Analysis and Rejection of WAPI Ballot Comments:

A Supplement to China's appeal document Unjust Activity, Undue Process, Unfair Results: Ethical and Procedural Violations in WAPI-11i Fast-track Process submitted on April 29, 2006 to ISO/TMB IEC/SMB

Chinese National Body

May 15，2006

Note: This document is prepared by Chinese National Body and presented to ISO/IEC Central Secretariats and TMB/SMB as a supplement to the document entitled **Unjust Activity, Undue Process, Unfair Results: Ethical and Procedural Violations in WAPI-11i Fast-track Process** which has been submitted to ISO/IEC central offices on April 29, 2006. This document may also serve as preliminary analysis and response to WAPI ballot comments to SC6 Secretariats to be distributed to national bodies before the June meeting. Attachment is a document compiled by Chinese NB on Nov. 30, 2005 in response to the comments received during the Sept. 7-Oct. 7 about the perceived contradictions between WAPI and 11i proposals.

1. Introduction

On April 29, Chinese National Body (SAC) formally submitted an appeal document to ISO/IEC Central Secretariats. The document points out that there were extensive ethical and procedural violations in the WAPI-11i fast track ballot process and therefore the ballots results are unfair and unacceptable. Because the issues are extensive, involve a lot of principles and cannot be resolved within JTC1 system, ISO/IEC central management offices are requested to take immediate actions to resolve important issues facing the two proposals.

Now that China has completed analyzing the ballot comments on WAPI. Several important conclusions can be made. The following report will demonstrate that the

concerns and complaints expressed in April 29 appeal document are legitimate, that the negative comments against WAPI are factually or procedurally false and therefore are unjust and unacceptable, that the negative votes against WAPI are unfair and unacceptable, and that neither the BRM nor the normal JTC1 dispute settlement process are the proper mediums to resolve the issues.

2. Ballot Comments Summary

2.1. Some facts:

There are about 17 NB's voted against WAPI and provided ballot comments.

The majority of comments are brief.

The most extensive comments provided were submitted by ANSI.

The ANSI comments are identical to the documents produced by IEEE during the comment and ballot period.

The issues raised in the ballot comments do not go beyond the scope covered by the IEEE documents.

Some national bodies either directly copied comments from IEEE document or cited the IEEE document as the ground for rejecting WAPI.

Although there were numerous comments in the ballot documents, there were only 11 issues at dispute.

2.2. The Issues

Issue #1. 1N7904 is not complete in technology and the proposal deletes description for some algorithms on purpose, including the details for Block Cipher algorithm. The encryption algorithm should be submitted to the ISO/IEC standardization process together with the WAPI technical concepts. The lack of at least one mandatory, disclosed block cipher makes it impossible for vendors world wide to build interoperable implementations that work globally, which is the whole purpose of an international standard.

Issue #2. The certificates and Protocol Groups defined in 1N7904 are out of scope of any ISO/IEC 8802 standard. The proposal causes both structural and technical problems.

Issue #3. The proposal of 1N7904 deletes WEP security mechanism, so it could not supply backward compatibility with deployed devices and forward compatibility of other IEEE standard.

Issue #4. There are editorial and grammatical errors in the proposal of 1N7904.

Issue #5. There exist editorial conflicts in 1N7904 and 1N7903 (IEEE 802.11i on security), and they could not be harmonized as the supplement of ISO/IEC 8802.11. Therefore, WAPI should be rejected.

Issue #6. There are security defects in 1N7904: the inducing way of BKID and key negotiation uses challenge.

Issue #7. 1N7904 does not have the qualification of ISO fast track. Especially, it is pointed out that, ISO/IEC standards are irrelevant unless they achieve global acceptance and wide deployment. But 1N7904 is devoid of wide deployment.

Issue #8. Some questions raised are result of misunderstanding of the document of 1N7904.

Issue #9. Doubt about Patent statement in WAPI.

Issue #10. WAPI did not follow IEEE-SC6 Agreement

Issue #11. More time need for consultation and harmonizing with 11i.

3. General Analysis

Analysis of the ballot comments reveal that the ethical and procedural problems also exist in the ballot period. Some of the problems have already been covered in the April 29 appeal document, but there are more problems need to be reviewed and resolved.

3.1. Comments Raising Procedural Issues

Among the 11 issues, 10 concerns procedures (1-5 and 7-11). Only issue #6 is technical which is easy to be answered. The major theme in those comments is that WAPI is not qualified for Fast Track process.

Some comments are purely procedural with no technical discussions. Some comments are technical related, but because those technical issues have already been considered in previous procedures that raising them again in the ballot would create procedural conflicts.

3.2. Using procedural reasons against WAPI

Those procedural issues have been discussed in numerous meetings during July 2004 and September 2005. IEEE had used the arguments during that period to prevent WAPI from entering the fast track process. The fact that WAPI had entered the fast track process on Sept. 6 and ballot on Oct. 7, 2005 through a series of decisions should establish the principle that the procedural objections can not be used as ground for negative votes against WAPI.

3.3. Ignoring China's Responses

During the pre-fast track discussion period, China has provided numerous and detailed responses to those procedural issues. China's documents have not only answered questions and provided explanations, but also proved that the objections cannot stand against careful reasoning and lack support from ISO/IEC rules of principles.

However, the ballot comments ignore China's responses, but insist on original arguments which have already been refuted.

3.4. Ignoring Previous Decisions

Many of the arguments have been discussed in previous meetings and many official decisions have been made against them. However, those arguments appeared again in the ballots and are used as grounds to vote against WAPI.

Official decisions have been repeatedly and continuously ignored or violated.

3.5. Reversing Positions Repeatedly

We are seeing National Bodies making self-contradicting positions. For example, there is a NB which objected WAPI processing in ISO/IEC in summer 2004, later agreed to modify position to allow WAPI go through fast track within ISO/IEC in the fall of 2004, but then in the ballot reversed position again to demand China submit WAPI to IEEE for processing.

3.6. Blaming the Victim

The ballot comments demonstrate a “blaming the victim” approach. WAPI is the victim of procedural violations, but it becomes the target of criticism and punishment.

For example, China had proposed to form editorial groups to edit WAPI and 11i for final approval in Beijing meeting and France meeting, but the suggestion was turned down by IEEE. Lately, IEEE claimed that WAPI should be rejected because it needs editorial work in its document. Now, there are some National Bodies copy the word one-to-one from IEEE document.

3.7 Double standard

The ballot comments also demonstrate double standards are used in vote on WAPI and 11i.

For example, both WAPI and 11i need editorial work. However, WAPI was singled out for rejection despite that 11i has similar work to be done.

Also, two national bodies submitted two proposals which might have contradictions, but one NB’s proposal (11i) was selected for approval, but the other NB’s is singled out for rejection on the ground that it “contradicts with the other proposal”.

3.8. Ignoring the Utmost Important Factor

The two proposals are amendments to fix the security loopholes of the base

standard ISO/IEC 8802-11. Therefore, the utmost important factor in considering the proposals should be the security performance.

However, the ballot comments focus on minor and procedural issues but fail to see the technical and structural strength of WAPI.

On the other hand, 11i has numerous technical defects and poses serious security risks. But, the ballots totally ignore these issues.

3.9. WAPI Technical Strength

The ballot comments raise no serious technical challenges and exposed no security or structural weakness in WAPI technology. Considering 11i's evident security defects and structural weakness, China is fully confident that WAPI is the best available security solution for WLAN and should a bright future in world-wide application.

3.10 Ballot Comments are Unacceptable

China has studied the ballot comments against WAPI, taking into account the 11i situation, and found that none of them is sound argument; that none should be used to reject WAPI; none is fair and reasonable; and that none can be accepted.

3.11 1N7903 (11i) should be Referred Back to WG

The ballot comments also strengthen China belief that 1N7903 (11i) is not qualified for International Standardization. Theoretically, both proposals can coexist in one standard as alternatives. But WAPI can provide the best and more reliable security protection while 11i has numerous defects. 11i needs to be referred back WG to fix its problems. So, WAPI is the only remaining choice for adoption.

3.12. Addition of Appeal Issues

The following will be a detailed analysis of the issues raised in ballot comments. It will demonstrate that the April 29 appeal did not cover all the issues need to be settled.

The new issues will be summarized in section 5.

4. Issue Analysis and Disposal

Issue #1. Disclosure of Algorithm

1N7904 is not complete in technology and the proposal deletes description for some algorithms on purpose, including the details for Block Cipher algorithm. The encryption algorithm should be submitted to the ISO/IEC standardization process together with the WAPI technical concepts. The lack of at least one mandatory, disclosed block cipher makes it impossible for vendors world wide to build interoperable implementations that work globally, which is the whole purpose of an international standard.

4.1 China Response to Issue #1: Reject.

Analysis:

- This is not a new issue.
- This involves procedures.
- China has provided explanations and answers many times before the ballot period.
- WAPI's treatment of algorithm complies with ISO/IEC related rules and principles.
- The criticism on WAPI about algorithm is unfair and has no factual or procedural basis.
- It has been included as an issue to be resolved in the April 29 appeal document.
- On the other hand, 11i's treatment of algorithm is problematic.

Further Action desired:

The algorithm issue is significant and has to be resolved by ISO/IEC central management offices. China is looking forward to have an opportunity to work with ISO/IEC leadership to completely resolve the issue.

Issue #2. Out of Scope

The certificates and Protocol Groups defined in 1N7904 are out of scope of any ISO/IEC 8802 standard. The proposal causes both structural and technical problems.

4.2 China Response to Issue #2: Reject.

Analysis:

- This is not a new issue.
- This is a procedural issue.
- China has provided explanations and answers many times before the ballots.
- The criticism on WAPI about scope is unfair and has no factual or procedural basis.
- WAPI's inclusion of certificates and protocol groups are legitimate and does not violate ISO/IEC rules of procedures.
- The argument of disintegrating WAPI and standardizing it in other organizations is absurd and unacceptable.

Further Action desired:

This issue was not included in the April 29 appeal. This is an important issue, as it involves many issues including procedural and principles and has impact on how security standards are to be made in the future.

China wishes this issue be added to the appeal list so that it is completely settled and no similar confusions will happen again.

Issue #3. Backward and Forward Compatibility

The proposal of 1N7904 deletes WEP security mechanism, so it could not supply backward compatibility with deployed devices and forward compatibility of other IEEE standard.

4.3 China Response to Issue #3: Reject.

Analysis:

- This is not a new issue.
- This is a procedural issue.
- China has provided explanations and answers many times before the ballots.
- The criticism on WAPI about backward and forward compatibility is unfair, unjust and unacceptable.
- China points out that deleting WEP has just reasons.
- It is for better security.
- 11i retains WEP and thus prolongs and create more security problems.
- Backward compatibility is not an excuse to downgrade security performance and it should not be used as a reason to reject an advanced and reliable solution.
- Backward compatibility can be done by upgrades to old systems.
- Even though 11i contains WEP with all the old and newer security loopholes, the newer functions introduced in 11i will still create backward compatibility and interoperability problems and will demand upgrades in old systems.
- Therefore, retaining WEP is an unwise and insecure approach.
- China will never agree to allow an outdated and defected technology to weaken the security protection in WAPI technology.
- Regarding forward compatibility, it has been discussed in Geneva meeting and the issue has been resolved. WAPI does not prevent forward compatibility with IEEE standards.
- Therefore, neither argument can be used to reject WAPI.

Further Action desired:

The backward and forward compatibility issues are not included in the April 29 appeal. China desires to add these issues to appeal list because these issues involve procedures and have been discussed in levels over JTC1 process such as the Geneva meeting.

Issue #4. Editorial Issues

It was claimed that WAPI is immature and should be rejected because there are editorial and grammatical errors in the proposal of 1N7904.

4.4 China Response to Issue #4: Reject.

Analysis:

- This is a procedural issue.
- WAPI has been unduly blamed and singled out for discrimination.
- Grammatical errors do not reduce the technical strength.
- 11i and WAPI should be treated on an equal basis.
- This has been included in the April 29 appeal.

Further Action desired:

This issue should be dealt with in the appeal process. 11i's editorial issues should also be considered.

Issue #5. Editorial contradictions with 11i

There exist editorial conflicts in 1N7904 and 1N7903 (IEEE 802.11i on security), and they could not be harmonized as the supplement of ISO/IEC 8802.11. Therefore, WAPI should be rejected.

4.5 China Response to Issue #5: Reject.

Analysis:

- This is not a new issue.
- This is a procedural issue.
- The contradictions should not be used to reject WAPI.
- WAPI is unfairly discriminated against.
- The argument violates the procedures.
- This issue has been included in the April 29 appeal.

Further Action desired:

This issue should be dealt with in the appeal process. 11i's contradiction with WAPI should also be considered. The discrimination against WAPI is unfair and unjust.

Issue #6. Alleged Security Defects in WAPI

There are security defects in 1N7904: the inducing way of BKID and key negotiation uses challenge.

4.6 China Response to Issue #6: Reject.

Analysis:

- This is a technical comment.
- But it can be easily explained.
- BKID: BKID is used to indicate if the current BK changes and would not bring any security threat. WAPI is designed with careful and full consideration of avoiding possible attacks. In fact, the method adopted in IEEE 802.11i is the same as 1N7904 on this point.
- Key negotiation challenge: attackers have to intercept AE frames firstly and then re-send them. But if the negotiation that AE initiated is not completed, the secure association between AE and ASUE would be closed, and AE and ASUE would delete USKSA, so this challenge is no

longer valid and the replay attack doesn't effect.

- Therefore, the alleged security defects in 1N7904 are not tenable.

Further Action desired:

None.

Issue #7. Qualification for fast track

It is claimed that 1N7904 does not have the qualification of ISO fast track. Especially, it is pointed out that, ISO/IEC standards are irrelevant unless they achieve global acceptance and wide deployment. But 1N7904 is devoid of wide deployment.

4.7 China Response to Issue #7: Reject.

Analysis:

- This is a procedural issue.
- This kind of comment challenges previous decisions by SC6 2004 and 2005 plenary meetings, by ISO/IEC Central offices and by ITTF.
- The interpretation of "fast track qualification" is problematic.
- The same arguments could be used against 1N7903 as well.
- It is unacceptable.

Further Action desired:

This issue has not been mentioned in the April 29 appeal. China wishes to add the issue to the appeal issue list. The questions are: what are qualifications for fast track. Does WAPI qualify fast track? Because the issue challenges ISO/IEC central secretariats and ITTF decisions, it must be resolved by ISO/IEC central management offices.

Issue #8. Misreading 1N7904

Some comments in ballots are the results of misreading the 1N7904 and causing

technical questions.

For example, some national bodies pointed out that, the text states “there are two USKSAs at most…both may be active during rekeying process.” This description is incompatible with the USKSA data structure defined on page 28. In particular, the KeyIdx used by WPI to identify the USK is missing.

4.8 China Response to Issue #8: Reject.

Analysis:

- This is a misreading of the document.
- In fact the so-called question is an illustration of lack of knowledge on 1N7904. On page 28 of 1N7904, the USKSA data structure is defined to include USKID to identify the USK, and on page 66 the KeyIdx used in WPI indicates the USKID, MSKID, or STAKeyID. So the relationship between USKID and KeyIdx is very clear in context of 1N7904.
- As a result, the statement of “the KeyIdx used by WPI to identify the USK is missing” is false.
- Such comments cannot be used as grounds to reject WAPI

Further Action desired:

We suggest more careful reading of WAPI documents and contact China NB for technical clarification and consultation.

Issue #9. Doubt about Patent statement in WAPI.

The Chinese NB has proposed 1N7904 (WAPI) as an amendment to ISO/IEC 8802-11. 1N7904 contains an IPR statement in relation to WAPI offering RAND (Reasonable and Non Discriminatory) terms. If 1N7904 (WAPI) was approved as an amendment then the resulting ISO/IEC 8802-11 standard would not longer be substantially similar to IEEE 802.11. In this case, it is

doubtful that any of the IPR statements (also offering RAND terms) made to the IEEE in relation to IEEE 802.11 would apply to the version of ISO/IEC 8802-11 amended by 1N7904 (WAPI).

The text provides information on China specific patents. This leaves open a question whether there are further patents which need to be disclosed.

4.9 China Response to Issue #9: Reject.

Analysis:

- This is a procedural issue.
- The patent is an issue that handled by ITTF and China.
- China has provided patent information to ITTF according to procedural requirements.
- ITTF is satisfied with WAPI's patent documentation.
- Therefore, the patent question cannot be used to vote against WAPI.
- Any question regarding 8802-11 patents should be directed to other places for discussion.
- Opposition against WAPI based on patent confusions is not an acceptable ground for rejection.

Further Action desired:

This procedural issue was not included in the April 29 appeal document. China wishes to add this issue to appeal list. The questions are: Does WAPI proposal violate patent procedures and can NB use patent issues to reject WAPI?

Issue #10. IEEE-SC6 Cooperation Agreement

Any action which ISO/IEC takes towards publication may severely impact upon the existing agreement that existing with the IEEE Standards Board with respect to existing and future output from the

IEEE 802 Committee. The UK considers this would not be in the best interests of any stakeholders of the standards making process. If this proposed amendment is approved, it will create a precedent whereby a mechanism for setting up an alternative LAN standardization process is established which disregards the close, documented, working relationship built over many successful years between IEO/IEC and the IEEE 802 Committee, and which may subsequently be invoked where there is disagreement with existing and developing IEEE LAN standards. The UK considers this precedent would not be in the best interests of any stakeholders of the standards making process.

4.10 China Response to Issue #10: Reject.

Analysis:

- This is a procedural issue and a very old issue.
- China is surprised to see such comment at this stage, especially from a NB which has representatives in most of the WAPI-11i meetings in 2004-2005.
- This issue has been discussed extensively in previous meetings.
- The arguments have been presented before and have been rejected several times.
- UK had made this argument in August 2004 and had given up the argument in Orlando meeting. It is a surprise to see the reemergence of this argument in the ballots.
- This argument is factually and procedurally false.
- This argument violates previous decisions and resolutions.
- This argument cannot be used to reject WAPI.
- This issue has been included in April 29 appeal document.

Further Action desired:

The April 29 appeal document included the issue of controversy surrounding IEEE-SC6 agreement and the repeated demand of submitting WAPI to IEEE for processing. China reaffirms the position that the issue been resolved by ISO/IEC central offices completely and resolutely. The questions are: Did WAPI violate the IEEE-SC6 agreement? Are this kind of changing positions and repeated demands constitute procedural violations?

China has declared positions and provided explanations many times in the past and will continue to cooperate with ISO/IEC central offices and related parties to solve any lingering confusions and disputes.

Settling this issue would not only help resolve the WAPI-11i controversy, but also will prevent future confusions and controversies on similar issues.

Issue #11. More time needed

Some national body voted against WAPI with comments that more time is need for consultation and for harmonizing with 11i.

4.11 China Response to Issue #11: Reject.

Analysis:

- This is a procedural issue.
- WAPI is singled out for rejection while 11i got favorable votes despite its technical and editorial problems.
- Differential treatment of WAPI and 11i violates ISO/IEC code of ethics and rules of procedures.
- The arguments against WAPI are not on legitimate grounds.
- There are misinterpretations about harmonizing.
- Harmonizing should not be used as a ground to approve 11i and reject WAPI.
- There is urgent need for enhanced security solutions.
- WAPI is the most advanced, more reliable, more secure and most

efficient security solution available now.

- Delay WAPI's international standardization and world-wide application is an irresponsible, unfair and unacceptable behavior.
- Forcing 11i into International standardization despite its inherent and evident defects is also an irresponsible and unjust behavior.

Further Action desired:

The issue of harmonizing WAPI with 11i has been discussed many times before the fast track process. China had presented our views and positions. The issue did not prevent WAPI from entering fast track. But now, the argument is used as ground to reject WAPI. But the April 29 appeal did not include itself as an issue for appeal.

Therefore, China wishes to add this issue to appeal issue list. The question is: can harmonization be used as grounds to reject WAPI? Is it legitimate to single out WAPI for rejection based on harmonization argument?

Another related issue needs to be considered is that there were obvious attempts to delay WAPI processing in the past and continued attempt to use harmonization as an excuse to delay the application indefinitely. This kind of behavior violates the "provide timely standards" and "prevent unnecessary delay" principles of ISO/IEC.

China wishes to call ISO/IEC central office's attention to this matter and to take actions to prevent intentional delays and find ways to satisfy the world-wide urgent need for new solutions to fix the security loopholes in WLAN systems.

4.12 Summary

Analysis of the ballots and comments indicate that all the negative ballots and comments against WAPI are questionable and lack factual, procedural and/or technical basis. Therefore, the ballot results are unfair, unjust and unacceptable.

China believes that the issues cannot be resolved in the BRM meeting, or within the JTC1 system. The only hope for successful settlement is the intervention of ISO/IEC central management and supervisory offices.

5. On the issue of 11i and BRM

5.1. The fact that little attention was paid to the numerous technical problems and editorial errors in 11i in the ballots and comments on 1N7903 is startling and very troublesome, especially when compared with what kind of arguments and attention has been paid to WAPI.

5.2. Rejecting WAPI for minor procedural questions which cannot stand against careful analysis and reasoning, while in the mean time approve 11i despite its inherent and serious security defects is also puzzling and unfair.

5.3 There are strong and abundant evidences to demonstrate 11i's technical defects and structural weakness. It can not fix the WLAN security loopholes and there is no short fix to 11i's defects.

5.4 The editorial problems are also numerous and undeniable. (According to SC6 distributed document, PE of 11i has agreed with China that there were numerous technical and editorial problems within 11i. Although PE has rejected some China's technical comments, the grounds of rejections are also very weak and problematic. See 6N13082).

5.5 Therefore, 11i is immature and the only viable path is to refer it back to WG as the ISO/IEC directives mandate.

5.6 Therefore, the BRM meeting on 11i is unnecessary and should be cancelled.

5.7 It is utterly irresponsible for the Project Editor of 11i admitting the existence of numerous technical and editorial defects and the fact that there is no short fix to the technical problems in 11i, but at the same time recommending its "publication without modification" on the ground that it has won approval votes. Such recommendation violates the ISO/IEC Directives as discussed in China's April 29 appeal document.

5.8 The PE disposal should be added to the list of issues for appeal.

6. Suggested Actions

6.1 China reaffirms the positions and demands expressed in the April 29 appeal document.

6.2 China repeats the request for ISO/IEC central offices and TMB/SMB to study and resolve the issues listed in the appeal document.

6.3 Furthermore, China wishes to add the following issues to the appeal list:

6.3.1， Additional Appeal Issue #1: Did WAPI extends over the scope?

6.3.2， Additional Appeal Issue #2: Does WAPI has to retain WEP?

6.3.3， Additional Appeal Issue #3: Does WAPI prevents forward compatibility with IEEE standards?

6.3.4， Additional Appeal Issue #4: What qualifies for fast track process? Does WAPI qualify for fast track?

6.3.5， Additional Appeal Issue #5: Does WAPI proposal violate patent procedures and can NB use patent issues to reject WAPI?

6.3.6， Additional Appeal Issue #6: can harmonization be used as grounds to reject WAPI? Is it legitimate to single out WAPI for rejection based on harmonization argument?

6.3.7， Additional Appeal Issue #7: There were intentional delays for WAPI international standardization.

6.3.8， Additional Appeal Issue #8: How to quickly fix the security loopholes in existing WLAN standards thereby satisfy the urgent need for advanced and reliable WLAN security solutions.

6.3.9， Additional Appeal Issue #9: 11i PE editor’s recommendation for 11i publication violates ISO/IEC Directives.

6.4 Because the WAPI ballots and comments are subjects for appeal and the disposal relies on the results of the appeal, the WAPI BRM meeting is not necessary and should be indefinitely postponed until the procedural confusions and principle issues are completely resolved.

6.5 Any attempt to resolve the dispute by forcing votes in BRM meeting and therefore disregard China’s rights and call for fairness, justice, due process and consensus would be unfair and unacceptable.

7. Conclusion

WAPI ballot and comment analysis supports what have been presented in China April 29 appeal document. Not only the issues and complaints are legitimate, but also additional issues for appeal have been identified.

Above the discussions further support China's view that there were unjust activities, undue process, unfair comments, unreasonable ballots, and therefore the results are unacceptable.

China rejects all the anti-WAPI ballots and comments because they are unfair, unjust and unacceptable.

China restates the view that the BRM for both WAPI and 11i are unnecessary. WAPI ballots and comments are subjects of appeal and should be resolved through the intervention of ISO/IEC central management and supervisory offices. 11i's BRM is also unnecessary because it must be referred back to WG according to the directives as it is now very clear and evident that it has numerous technical defects and editorial problems.

China requests that all the issues listed in the April 29 appeal document and in this supplemental report are carefully and thoroughly investigated and studied. The issues should also be definitely resolved with clear and written conclusions and instructions. No ambiguities should be left behind because we have seen what kind of confusions, delays and controversies will result from it.

China welcomes any suggestions on how to move forward with the WAPI proposal. China is committed to work with all national bodies and related parties to make WAPI the advanced and reliable solution available to the international community to help fix the existing WLAN security problems.

Attachment: **China's Response to Contradiction Comments on 1N7904** （Chinese National Body, Nov. 30, 2005）

Attachment:

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/SC6 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 offices, JTC1 and SC6 secretariats and other related parties for their reference. It is understood that because the proposals covered in this correspondence has entered balloting 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 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.'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: 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: 1 N 7904 (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: 1 N 7904 (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: 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.

Issue 6: 1 N 7904 (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: 1 N 7904 (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: 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 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	German	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 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 in this document answer again those questions in detail. 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 and Chinese national body has provided detailed response to it.[1]

2) WAPI has gone through extended reviews.

From August 2, 2004 to Sept. 6, 2005, WAPI has gone through an

[1] "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status" and 1N12960 "notes from Chinese national body" (August 31, 2005, Beijing Meeting).

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 Secretariats 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 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) WG1 special meeting
- May 17, ISO/IEC special work group meeting in Geneva

(Switzland)

- 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, 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

[3] SC6 2005 plenary meeting resolutions, 6N12765

[4] *"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 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

- In Geneva 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]
- In Beijing meeting, 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 headquarters that WAPI will enter ballot with 11i on October 7, 2005. This is a sound and wise decision.

---

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 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.*"

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 tried very hard to comply 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 FT 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 Beijing meeting.

2) We have explained before.

Answer to this question was provided by the Chinese delegation in SC6 2005 France (St. Paul De Vance) plenary meeting. In document entitled "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status," 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 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:

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.

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

[7] JTC1 Directives, page 56.

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 错误！未找到引用源。 an SC may suspend normal processing in favour 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 headquarters 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

[8] JTC1 Directives, page 62.
[9] JTC1 Directives, page 71.

"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 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

[10] JTC1 Directives, page 46.

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, 1 N 7904 (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.

For more details, please see "WAPI-CHN-T106_Response to Comments on WAPI".

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 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

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

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

[12] For more Chinese comments on 11i, please see JTC1 document "Compilation of National Body Comments on JTC 1 N 7903, 30 Day Review for Fast Track Ballot ISO/IEC DIS 8802-11/Amd.6".

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.
- We have consulted senior ISO/IEC officials on this matter.

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 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 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

[13] See documents entitled "SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status" and "WAPI-CHN-T106_Response to Comments on WAPI".

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 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

[14] See detailed analysis on “CNB comments on 11i” presented at SC6 France plenary meeting on August 31-Setp.2, 2005.

protect the interests of consumers and communities, making this kind of trade off and compromising security is an irresponsible behavior. Future WLAN market is hundreds or thousands 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, Beijing 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 resolution 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 resolution 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

15 SC6 Orlando Resolution # 6.1.10, Nov. 12, 2004

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 headquarters 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 did not request WAPI to comply with 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

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

to settle the issue permanently. [17]

Issue 8: WAPI Cryptographic Algorithm 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 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 algorithm. [18]

In SC6 2005 plenary meeting in France, August 31-Sept. 2, 2005, Chinese NB further explained the issue in document reviewing the

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

[18] ISO/IEC Central Secretariats document WAPI N 33.

status of the WAPI proposal".[19]

2) There is no international standard in cryptographic algorithm.

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

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

5) Cryptographic algorithm has sensitive political and security implications. There are laws and regulations governing cryptographic algorithm in many nations. International standards should not supersede those laws and regulations but instead should allow compliance with them.

6) WAPI only defines a security protocol and does not mandate any cryptographic algorithm. The security protocols and cryptographic algorithms are independent from each other. WAPI lists SMS4 algorithm as an optional reference. According to local regulatory requirements and needs, different algorithms such as AES, TWOFISH or SEED etc. can be selected or implemented. The listed optional algorithm SMS4 is owned by Beijing Data

[19] See "WAPI-CHN-T708-Encryption issue" and "Status Review of WAPI Proposal" （SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status）

Security Technology Co. Ltd. (BDST). For more information, please contact BDST at: chinabdst@126.com. Therefore, WAPI does not impose any algorithm 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 algorithm does not violate any ISO /IEC standardization rules.
9) The request for more openness of SMS4 algorithm 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 in China. 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 in 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 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 constitute 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 security.

Chinese government has an obligation to provide a secure environment for our nation. China cannot accept anything which would

[20] Chinese national body, "Status review of the WAPI Proposal, August, 2005, presented to SC6 2005 plenary meeting.

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. There 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 obvious serious defects of the other proposal.
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.