Preliminary Response to IEEE Comments on 1N7904

Chinese National Body (SAC)

February, 2006

On November 2005, IEEE published its comments on ISO/IEC JTC 1N7904 (Chinese WAPI proposal) in ballot procedure. However in fact, most of their questions had been discussed and clarified in previous many international standard conferences (including SC6 Orlando plenary meeting in 2004, SC6/WG1 Frankfurt meeting, ISO/IEC WAPI Beijing special meeting, SC6 France plenary meeting in 2005, etc.), and at the same time, they has been fully explained in the letter “China’s Response to Contradiction Comments on 1N7904” sent to the ISO/IEC JTC1 National Bodies by Chinese National Body (SAC) in December, 2005.

In order to further clarify correlative problems, Chinese National Body classifies all the comments (414 items in total) into 9 aspects. The following is the Preliminary analysis and explanation on each aspect.

1, IEEE: 1N7904 is not complete in technology and the proposal deletes description for some algorithms on purpose, including the details for Block Cipher algorithm. (10 items)

Analysis：

The main body of the WAPI security protocol is fixed, with careful consideration of cryptography knowledge, and the cryptographic algorithms in them are optional and adoptable modules. Security protocol and cryptographic algorithms are relatively independent, and WAPI security protocol is applicable to multiple cryptographic algorithms. Cryptographic algorithms are only adoptable modules. Which algorithm to be applied is subject to the user’s requirement and national/ regional regulations.

1N7904 has different methods in dealing with cryptographic algorithms from 1N7903 (IEEE 802.11i). 1N7904 doesn’t force to adopt any specific cryptographic algorithms (including symmetric algorithm and the parameters of ECC), even China’s algorithms. In 1N7904, which algorithms to be applied are optional. Every national body can choose specific algorithms according to requirement and local regulations, and this makes ISO standards furthest applicable without any barrier.

Certainly, if there is a will, it is OK for other countries to use the China’s algorithms.

The Annex I (informative) of 1N7904 gives the way of how to get the algorithms: “The detailed information can be obtained from Beijing Data Security Technology Co. Ltd. (BDST). (E-Mail: chinabdst@126.com).”

It is worth noting that Chinese National Body (SAC) provided a detailed written reply for this issue on Beijing meeting (please see the file *N_33_WAPI_and_Cipher_issue_by_CNB_Beijing_Meeting_8-12_August_2005.pdf* for details) and SC6 French plenary meeting (see *SC6 WG1-CHN-003-WAPI Status.doc*). WAPI proposal is fully conformed to ISO/IEC regulations and principles. We consider this issue has been resolved properly.

2, IEEE: the certificates and Protocol Groups defined in 1N7904 are out of scope of any ISO/IEC 8802 standard. (11 items)

Analysis:

WAPI is an advanced and creative security mechanism designed for WLAN and its feature is peer access control and mutual authentication. WAPI solves the problems caused by WEP and it is an integrated solution. In addition, many state machines in WAPI are controlled by MAC protocol, and WAPI and MAC protocols have become an integrated part. WAPI implements the security of MAC layer, and certificate mechanism adopted in WAPI is just a way to implement the MAC layer security. So it should be in scope of ISO/IEC 8802 of SC6 WG1.

On the other hand, the 4-way handshake protocol and the STAKey handshake protocol are defined in IEEE 802.11i, and the packets of these protocols are carried in the data frames of MAC layer as the WAPI protocol packets. According to the logic of IEEE, if WAPI goes beyond the scope of the ISO/IEC 8802 standards, the 4-way handshake protocol and the STAKey handshake protocol of IEEE 802.11i DO NOT belong to layer 1 and layer 2 specifications, and are not within the scope of SC6 WG1.

Furthermore, 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. Then according to the same logic of IEEE, IEEE 802.1x should be beyond the scope of SC6/WG1. Furthermore, IEEE 802.1x is just an internal standard of IEEE, not an international standard until now. Is it necessary for IEEE to submit IEEE 802.1x to ISO/IEC for ballot firstly, and then adopt it in IEEE 802.11i when approved?

From this point, is it a fact that IEEE 802.11i does not satisfy the requirements for the ISO/IEC proposal? It is well known that IEEE has higher industry level and is quite familiar with the requirements of the international standards. But, why do they propose this proposal? And is it on purpose?

If IEEE 802.11i does not include the technologies beyond the scope of SC6 WG1, then WAPI, which is designed specifically for WLAN to resolve security problem of WEP in ISO/IEC 8802-11, should be within the scope of SC6 WG1.

It is worth noting that Chinese National Body has proposed documents in Beijing meeting and France meeting about this issue.

3, IEEE: the proposal of 1N7904 deletes WEP security mechanism, so it could not supply backward compatibility with deployed devices. (14 items)

Analysis:

There are many security defects in WEP and it is easy to be cracked. WEP, which is still adopted in IEEE 802.11i, though not encouraged, still exposes WLAN users and networks in security risks. The defects of WEP are well known, a little of which can be found in the following web pages: http://www.winlab.rutgers.edu/pub/docs/JesseWalker.pdf and http://www.cs.umd.edu/~waa/wireless.pdf.

For the sake of information security and on behalf of users, WAPI does not provide backward compatibility to WEP and therefore maintains the highest level of security. WAPI is the best choice of manufacturers, who want uncompromised and reliable solutions, are willing to make their best to assure the basic requirement of user, industry and market, and are willing to be responsible for interests of international community and numerous users at the same time.

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

It is worth noting that, Chinese National Body has proposed documents in Beijing meeting and France meeting about this issue. It is fully thought over that WAPI does not provide backward compatibility to the old security mechanisms such as WEP, which satisfies the requirements of an uncompromised and reliable security mechanism.

4, IEEE: there are editorial and grammatical errors in the proposal of 1N7904. (232 items)

Analysis:

IEEE pointed out that, there are grammatical and syntactic errors in 1N7904.

However, we wish to point out that IEEE's attitude and behavior again violate ISO/IEC rules and principles, according to which, this kind of editorial issues should have been raised in early stages and editorial work should have been done by project editor and an editorial group. WAPI has been read, commented and revised for 18 months. Why IEEE waited until the ballot has started to raise these issues? And why the editorial group was not organized? Who has violated the ISO/IEC related policies? Why?

The answer is that IEEE has set up a language trap, waiting until the ballot has started so that the language issue can be used as a weapon to generate negative ballots against WAPI. And WAPI would be further delayed after the ballot. For this reason, IEEE turned down the proposal from China to form an editing group in Saint Paul De Vance meeting, August 2005.

5, IEEE: 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. (47 items)

Analysis:

This issue has been discussed specially at Beijing meeting in August, 2005, where Chinese NB submitted feasible solution for harmonizing two documents (N_32_Introduction_of_the_CNB_Contributions__Beijing_Meeting_8-12_August _2005.pdf), hoping the problem can be solved by the co-operation of both parties within three months. But IEEE refused to harmonize IEEE 802.11i with WAPI, insisting that it is impossible to finish the editing work in three months, and the protocol defined in WAPI be beyond the scope of ISO/IEC 8802 series. At the same time, IEEE changed the statement of "the two proposals are not mutually exclusive, both can reside in ISO/IEC 8802-11 as alternative and invoked when needed" at 2004 Orlando plenary meeting and claimed the two proposal are conflict and inconsistent, therefore the two proposals can not coexist and IEEE refused to harmonize with WAPI. At 2005 SC6 France plenary meeting, IEEE pointed out that, even though be approved by the IEEE delegation, the harmonization scheme proposed by Chinese National Body would not be approved by the engineers of IEEE.

According to the resolution of ISO/IEC central secretariat on September 6th ,2005, both 1N7904 and 1N7903 entered into fast-track procedure on September 7th. Chinese National Body always believes the two proposals could co-exist in international standards and could be harmonized into a single document. If possible, this issue could be solved by the discussion of Chinese NB, other national bodies and IEEE in the ballot resolution stage.

6, IEEE: there are security defects in 1N7904: the inducing way of BKID and key negotiation uses challenge. (6 items)

Analysis:

(1) 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 in the point.

(2) 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, it is untenable that there are the security defects in 1N7904.

7, IEEE: 1N7904 does not have the qualification of ISO fast track. (8 items)

Analysis:

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. At the same time, any well-meaning action should not be considered to be inconsistent with proposal procedure.

In fact, this kind of change shows Chinese National Body respects and welcomes any question and advice presented by national bodies and IEEE during the standard procedure. It is worth noting that so far no national body and no standard organization presents any doubt about the technology infrastructure of WAPI. At the same time, Chinese National Body has sufficiently considered and adopted all positive advices independent of WAPI technology infrastructure given by IEEE.

Therefore, the assertion “1N7904 does not have the qualification of ISO fast track” is not appropriate.

8, IEEE's understanding of the document of 1N7904 is not correct. (94 items)

Analysis:

There are 94 items of the document of 1N7904, which are understood incorrectly by IEEE.

For example, IEEE 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.* In fact the so-called question is a typical illustration of IEEE’s superficial 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.

These questions clearly indicate that, though WAPI is introduced into international community over 18 months, IEEE’s comprehension on technology and text of 1N7904 still stays on the surface. The reason is that IEEE has been devoid of positive and right attitude to 1N7904, and has been trying to exclude WAPI out of international community.

9, Doubt for the patent from IEEE (1 item)

Analysis:

The file of IEEE comments points out that, *as 1N7904 contains an introduction*

(identified as not being part of WAPI), the information contained therein is of note. As the introduction is not part of the balloted ISO/IEC 8802-11 Amendment, a complete China patent statement needs to be provided.

Whereas, the fact is that, when submitted 1N7904 on August 2005, Chinese national body submitted the China patent statement concerning 1N7904 to ISO/IEC at the same time according to the requirement of Patent Statement and Licensing Declaration of ISO/IEC/ITU. In the file, it is declared that, *the Patent Holder will grant a license to an unrestricted number of applicants on a worldwide, nondiscriminatory basis and on reasonable terms and conditions to use the patented material necessary in order to manufacture, use, and/or sell implementations of the above ITU-T Recommendation | ISO/IEC International Standard*.

So, the doubt doesn't exist since 1N7904 was submitted in August, 2005.

In summary, it is concluded that most of the IEEE's comments have been raised in many related international meetings held previously and have been explained and addressed by Chinese national body with great details in documents presented to those meetings. In the document, Chinese national body provides a preliminary reply to the questions raised by IEEE about 1N7904, and will make more detailed responses at the ballot resolution meeting.

WAPI provides a technical solution with strong security satisfying the requirements of wireless local area networks. So far, it is a flexible, manageable, and economical security mechanism, and the international community urgently needs such a security technology. Chinese national body has always welcomed any comment on WAPI.