Status View on WAPI Proposal

Chinese National Body
SC6 WG1 France Meeting, August 29, 2005

1. Summary

This document is prepared by the Chinese delegation for SC6 2005 Plenary Meeting, in St Paul De Vance, France. It provides an updated status report of the Chinese WAPI proposal. It describes the changes of the WAPI proposal since its introduction and documents the efforts of Chinese experts to modify the original proposal to make necessary changes to comply with International Standardization requirements. Special attention has been given to making the proposal compatible as much as possible with ISO/IEC 8802.11 and other relevant standards. This document will also provide reasons why some comments are not adopted.

Chinese National Body appreciates all the comments and suggestions from ISO/IEC Central Secretariats, SC6 National Bodies and liaison organizations such as IEEE. It is also our firm belief that the WAPI proposal, after extended reviews and changes, is now a mature proposal with advanced security mechanism and is fully qualified for ISO/IEC standardization.

2. WAPI Evolution and Comment Resolutions

WAPI Evolution:

In May 2004, Chinese NB voted against DIS 8802-11 and provided comments that included the whole contents of Chinese WAPI standard. (6N12687)

On July 26, 2004, Chinese NB submitted WAPI proposal to JTC1 and

SC6. It was given the number 1N7506 and started three month review.

On Oct. 15, Chinese NB notified JTC1 that it wants a fast track status for WAPI proposal.

Nov. 8-12, 2004, the fast track status of WAPI proposal was discussed in Orlando Meeting and it was confirmed that WAPI is qualified for fast track processing.

In Jan. 2005, JTC1 Secretariat determined that WAPI has satisfied one month review period and was ready for fast track balloting.

In May 2005, Geneva resolution adopted a double track approach, separating procedural issues from technical processing.

On July 2005, Chinese NB submitted ISO/IEC WAPI N16 which contains modified WAPI proposal as Part 1 for the purpose of forming a single joint proposal with IEEE 802.11i.

On August 25, 2005, Chinese NB resubmitted WAPI proposal to comply with the Geneva resolution.

Comments Received and Dispositions:

August 24 and 25, 2004, two letters raised objection to 6N12687/1N7506. Orlando Meeting resolved the issues.

In Jan. 2005, IEEE sent a response to SC6 and Chinese NB regarding 6N12687. The issues raised in that document have been resolved in Geneva meeting and Beijing meeting.

In Feb. 2005, IEEE provided detailed technical comments on WAPI proposal. Some changes are made to accommodate the comments and the results are reflected in N16 part 1.

In August 2005, IEEE provided some comments on WAPI as an independent proposal. Chinese delegation did not respond to those comments because it is beyond the scope of Beijing meeting. We will try to

resolve those comments in this document.

Conclusion: WAPI proposal has gone through extensive scrutiny and Chinese NB has made great efforts to accommodate comments.

3. 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.

4. Similarities and Differences between WAPI and 11i

Similarities:

Both proposals are intended to fix the same problem: security flaws in WLAN. Both are for fast track processing in ISO/IEC. WAPI and 11i are not mutually exclusive. They can both reside within ISO/IEC 8802-11 as alternative security mechanisms and implemented wherever is needed.

Differences:

WAPI becomes a standard one year earlier and was proposed to ISO/IEC one month earlier than 11i.

WAPI did not include WEP because of the need for a reliable and uncompromised security system.

WAPI has many technological advantages.

(A detailed technical comparison is available from Chinese Delegation.)

5. The Need for WAPI Technology

WAPI is a mature and feasible technology and it deserves to become an international standard.

- WEP has many well-known security problems, and it has been a obstacle to the development of international WLAN industry. WAPI provides innovative security technologies which are urgently needed by the international community.
- The technology accumulation on WAPI is more than 12 years. It successfully resolves all known WEP problems and possesses better security and performance than the other security mechanisms, including IEEE 802.11i.
- WAPI avoids compromising security for the sake of backward compatibility with flawed security mechanism. It avoids limiting the expansion of networks and avoids introducing any new attack points.
- WAPI has wide application beyond WLAN. WAPI technology can also be used in other fields, such as WMAN, WPAN, etc. Some companies have begun to develop WAPI compliant products of WMAN.

6. On Disclosure of Algorithm

A major criticism on WAPI is that it did not disclose algorithm. Chinese NB provided a detailed response to this issue in Beijing meeting. WAPI

proposal fully complies with ISO/IEC rules and principles in this regard. We believe that concerns on this issue have been adequately resolved. For more information, please refer to ISO/IEC WAPI N33.

7. On the Issue of Backward Compatibility

It is claimed that WAPI cannot be standardized because it does not provide backward compatibility while 11i does.

Chinese National Body points out that WAPI does not provide backward compatibility to the old security mechanism such as WEP like 11i does is based on careful consideration and satisfies the need of uncompromised and reliable security mechanism.

WEP has serious security flaws and is easy to crack. Allowing the technology, although its usage is discouraged, in WLAN systems would continue to put the WLAN users and networks under security risks.

International community needs an alternative security mechanism that is not compromised and provides the highest security protection. 11i contains WEP, while WAPI contains no WEP. Together, they form a complimentary system for the international community to choose according to local needs and requirements.

8. Options and Co-existence

China NB supports the concept of “one worldwide standard”.

However, one standard does not prevent alternative solutions.

International Standards should complies with national regulations and respect the concerns of national bodies.

ISO/IEC directives allow options.

WAPI and 11i are not mutually exclusive and both can reside within

ISO/IEC and be invoked according to local needs and requirements.

This is a position shared by both China NB and IEEE.

Therefore, WAPI's omission of WEP is an advantage rather than a weakness.

9. Splitting of WAPI Technology

There is an argument that WAPI proposal contains some elements that are not within the scope of SC6 WG1. It was suggested to split WAPI to extract some elements to standardize in SC6 WG 1, i.e., the elements of physical and data link layers. Whereas, the other elements should be standardized in other standardization organizations such as IETF and ITU.

In fact WAPI is an advanced and new security mechanism designed for WLAN, and the characteristics are peer access control and mutual authentication. WAPI addresses the problems caused by WEP. WAPI is an intact mechanism. Furthermore, The state machine of WAPI is controlled by the 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 means to implement the MAC layer security.

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. According to understanding of IEEE, 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. According to the understanding of IEEE, IEEE 802.1x is beyond the SC6/WG1. Furthermore, IEEE 802.1x is just an internal standard of IEEE, not international standard until now. Is it necessary for IEEE to submit IEEE 802.1x to ISO/IEC for ballot, then adopt IEEE 802.1x in IEEE 802.11i?

So, WAPI is designed specifically for WLAN to resolve security problem of WEP, and it should be in the scope of SC6 WG1.

10. WAPI's Qualifications

WAPI fully complies with ISO/IEC requirements for international standardization.

- China NB is eager to advance the industry development both in China and in other countries with advanced technology. As a P-member, China has right to submit WAPI to ISO/IEC directly and proceed WAPI in ISO/IEC structure.
- WAPI standard project was approved in 2001 and it became China's mandatory national standard in May, 2003 by AQSIQ (General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China).
- WAPI was submitted to ISO earlier than 11i. In July 2004.
- WAPI has been adopted and implemented in China more than one year before it was submitted to ISO/IEC.
- WAPI has been modified to satisfy ISO/IEC standard requirement.
- WAPI provides expansion capabilities.

11. WAPI Is a Mature Technology

- More than forty companies and institutions have taken part in the WAPI standard development process, including Chinese national standard and international standard proposals.
- WAPI provides a technical solution for maximum possible security. It is also a more flexible, more manageable and more economical solution.
- WAPI reduces the complexity of the implementation of products and reduce the complexity of management and maintenance of products.
- WAPI has 1.3 billion people consumer base.
- WAPI has been implemented widely in China. Many WAPI-compliant equipments have entered into services, including Wireless adapter, Access point, and Authentication server. WAPI's industry chain has become mature.

12. On Misalignment

There is a concern that if WAPI is adopted into ISO/IEC standards and published as an IS, it may cause misalignment with IEEE 802 standards.

Chinese NB believes that this is an issue not covered in the existing IEEE-SC6 agreement. Japanese NB made some comments on this issue when the agreement was considered in 2001. (SC06 N11861)

Chinese NB calls SC6 to start a review process to tackle this issue.

As this process will take time to complete, the current WAPI proposal should be handled with established general principles including:

ISO/IEC has the authority to publish International Standards.

No outside influence should delay ISO/IEC process.

No agreement should take away NB's rights in ISO/IEC.

The reciprocal principle should be applied.

According to these principles, WAPI should be considered within ISO/IEC and if adopted will be published as ISO/IEC standard. IEEE then is urged to readopt the approved WAPI into IEEE standard for alignment.

This approach was presented in Geneva meeting and was recorded in Geneva Meeting minutes, clause 64.

13. ISO/IEC Goals and Principles

In previous discussions, we have seen talks on ISO/IEC objective such as “one world-wide standard.” We have provided responses indicating that WAPI does not violate the one standard principle. Besides, WAPI should have more reasons to be adopted into IS if we take into account of other ISO/IEC goals and principles.

ISO/IEC standards are open standards.

ISO/IEC principles are against monopoly.

ISO/IEC has a goal of helping developing countries which include China.

ISO/IEC upholds the principle of fairness.

ISO/IEC develops responsible standards.

ISO/IEC standards take into account of national and regional regulatory differences.

ISO/IEC standards has performance requirement.

ISO/IEC has reciprocal requirements.

National Bodies needs to consider more than just business interests, but also public interests.

National Bodies have rights and obligations.

ISO/IEC standards should be suitable for adoption without change as a

regional or national standard.

Therefore, concerns from National Bodies should not be overlooked.

14. China's Positions

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 of 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.

15. Solutions

Chinese NB thanks all who have contributed to resolving the conflict. Let's us agree on a solution that is satisfactory to all. We can find a solution and we must find a solution.