Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 06 N12732

Date:	2004-10-18
Replaces:	
Document Type:	National Body Contribution
Document Title:	Letter from National Body of China to SC 6 regarding the Chinese proposal on ISO/IEC 8802-11.
Document Source:	National Body of China
Project Number:	
Document Status:	For discussion at the SC 6 Orlando meeting
Action ID:	FYI
Due Date:	
No. of Pages:	3

ISO/IEC JTC1/SC6 Secretariat
Ms. Jooran Lee, KSA (on behalf of KATS), Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ; Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : secretariat@jtc1sc06.org

Dear Ms. Jooran Lee,

In July 2004, ISO/IEC JTC1 Chinese national committee submitted a proposal based on Chinese current national standard GB15629.11 to ISO/IEC JTC1 and suggested it be adopted by Fast Track. The title of the proposal is "Information technology-Telecommunication and information exchange between systems-Specific requirement of LAN and MAN-Part 11: Wireless LAN media access control and physical layer specifications-Addendum 1: Specifications for Enhanced Security".

The JTC1 secretariat published JTC1 N7506 (see attachment 1) for reviewing our proposal on 2004-08-02. N7506 states: "This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, this project will be approved for addition to the SC 6 Programme of Work." But JTC1 announced "N7506 has been voided" and in a few days it published N7537 (see attachment 2) for reviewing IEEE 802.11i. Chinese national committee submitted its proposal according to JTC1 Directives. We think it would be better if JTC1 secretariat could have communicated with us and tell us the reason for canceling N7506 before it was cancelled.

Thus we hope that:

1. **JTC1 secretariat gives us the reason for canceling N7506 and communicates with us for how to consider our proposal.**

2. **International Standards should widely adopt the advantages of standards of all National Bodies. As a P-member of ISO/IEC/JTC1, Chinese national committee has obligation and right to participate in the development and maintenance of ISO/IEC/JTC1 standards. We are ready to make contribution to improving the standards. For this propose, Chinese experts deeply study the defects of DIS 8802.11 on security mechanism and radio transmission specifications for a long time, and GB15629.11 published in May, 2003 can solve the defects of ISO/IEC 8802.11: 1999. Based on GB 15629.11, we submitted our**

proposal "Information technology-Telecommunication and information exchange between systems-Specific requirement of LAN and MAN-Part 11: Wireless LAN media access control and physical layer specifications-Addendum 1: Specifications for Enhanced Security" to JTC1 according to JTC1 Directives. When ISO/IEC 8802.11:1999 is revised, JTC1 should consider the technology and experience of the proposal which is mature and has more contribution to Chinese market to improve the ISO/IEC 8802.11, so that the standard would be more perfect and more widely acceptable. So, we cannot understand why JTC1 secretariat announced N7506 has been voided soon after it was circulated.

Chinese experts have studies N7537 deeply and find several defects as follows:

1. No mutual authentication is specified in the standard and there exists a problem of lack of the user's confidence in network.

In N7537, the mutual authentication between AP and STA is implemented based on authentication process between STA and the authentication server (Radius), but it is not the really mutual authentication.

2. It is difficult to expand.

In N7537, a shared key must be set up for each AP and the authentication server manually, which leads to the bad expansibility. In a large-scale network, it is very difficult to manage the network.

3. Authentication protocol is complex in the standard.

The authentication protocol of N7537 is complex, and the authentication server is hard to expand.

4. There is a problem for the security of master key.

In N7537, the master key is produced by the negotiation between the mobile

endpoint and the authentication server, and the physical channel between the AP and AS transmits it. Therefore, it will bring new secure attack points.

To really improve DIS 8802.11 and to include more experience and technical advantages in it,

1. **We disagree to go through Fast Track Ballot on N7537 before seriously considering our proposal.**

2. **We suggest to discuss our proposal and N7537 among the delegates in the annual meeting of SC6 on Nov. 8~12. China delegation will attend the meeting and hopes to exchange with experts from other National Bodies.**

Guo Chen guang

Secretary, Chinese NC of IEC