Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N13863
Date:	2009-02-13
Replaces:	
Document Type:	National Body Contribution
Document Title:	NB of Switzerland's Comment on 6N13774 Draft of the WAPI standard
Document Source:	NB of Switzerland
Project Number:	
Document Status:	As per the SC 6 Montreux Resolution 6.1.5, NB of Switzerland submitted its comments on 6N13774.
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 : jooran@kisi.or.kr

Swiss Comment on 6N13774

As per SC6 Montreux resolution 6.1.5, 6N13774-13776 have been circulated for three months review and comment. This resolution was taken after consideration of 6N13719 and 6N13725, the latter document presenting the IEEE position on options 1-4.

The Swiss National Body prefers Option 3, i.e. the submission of WAPI as an International Standard, independent from ISO/IEC 8802-11, over the other options. The draft 6N13774 is a suitable starting point for the normal standardization procedure, which is the best way to address the various issues which we identified:

- Inconsistencies within the document
- Ambiguous and imprecise specifications
- Inconsistent and incomplete conformance requirements in the PICS.
- Concerns regarding compliance with the ISO/IEC patent policy
- Concerns in the area of privacy of personal information

Option 4, the TR option, is ruled out by the JTC1 Directives, section 16.2, as neither the criteria for type 1 (failed FCD) nor for type 2 (immaturity) nor for type 3 (other materials) are met. A type 1 TR may be considered later on, should WAPI fail in the standardization process.

The issues against Option 3 raised in 6N13725 cannot convince us:

1. Expertise & organizational memory required to modify 8802-11 not in SC6/WG1.
   This is not an issue for option 3, as it does not touch 8802-11.
2. Risk of setting the WAPI version up as an "orphan".
   a. The difficulty to synchronize WAPI with future editions of IEEE 802.11 can be overcome by the IEEE 802.11 WG closely involving ISO/IEC JTC1/SC6/WG1 into the maintenance of ISO/IEC 8802-11. SC6 should be the place where both standards, 8802-11 and the future WAPI IS, are maintained.
   b. IEEE fails to prove their claim that (cit.) "It is guaranteed that … WAPI ... will become an orphan …". WAPI has proven highly competitive, thus it may evolve independently from IEEE 802.11.
   c. In JTC1, competing standards are rather the rule than the exception, reflecting competition
   of technologies. Without such competition, there would be no progress. Competing standards are well accepted in JTC1. The citation of the ISO strategic plan is inappropriate, as JTC1 is a joint ISO/IEC body with its own directives, policies and business plans.
3. Not within the scope of SC6/WG1.
   WAPI specifies wireless communications with integrated security. The same objective has ISO/IEC 8802-11/Amd. 6, which was developed to overcome the security flaws of former WEP.

   Whereas JTC1/SC27 "Security Techniques" specifies generic security mechanisms, algorithms and requirements, WAPI and Amd.6 define how to use specific mechanisms and algorithms in conjunction with data communications. While this would certainly be out of scope of SC27, lacking the data communications expertise, it is well within the scope of SC6/WG1, capable to adopt the techniques developed by SC27.

   If not, then the Amd.6 is as well out of scope, and the newly launched fasttracks on NFC-SEC (6N13823-13824) defining a security layer on top of NFC (ISO/IEC 18092) too.

The Chinese contribution is welcome to complement the output of IEEE 802.11 WG, which has so far been the only source of related technology. We therefore invite the Chinese NB to submit a New Work Item Proposal, attaching an enhanced version of 6N13774 as a working draft. To obtain the approval of the Swiss National Body, an NWI proposal should provide satisfactory answers to the following questions:

- What is WAPI's differentiator? What does WAPI provide that cannot be as well achieved by TKIP-CCMP, or what does WAPI do better?
- What value does WAPI add to secure wireless communications, beyond WPA2?
- What market demand does WAPI satisfy?
- How can WAPI co-exist and inter-operate with ISO 8802-11 Amd 6?
- What features are negotiable?
- Does WAPI allow to negotiate CCMP?
- What features are required for conformance?
- How will the Chinese NB establish conformance with ISO/IEC patent policy?