Document Title: 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)

From: hittema tony, ht [tony.hittema@afnor.org]
Sent: Thursday, October 06, 2005 11:27 AM
To: RAJCHEL Liza
Cc: z60w@comelec.afnor.fr
Subject: French position on JTC 1 N 7409 "WLAN Authentication and Privacy Infrastructure (WAPI)"

Dear Liza,

This is to inform you that the French position regarding the JTC 1 Fast-Track proposal JTC 1 N 7904 on WLAN Authentication and Privacy Infrastructure (WAPI) is as follows:

In accordance with the JTC 1 Procedures, clause 13.4 on 30 day review period during fast-track, AFNOR has identified contradictions between JTC 1 N 7904 and existing ISO/IEC standards. In particular, JTC 1 N 7904 contradicts:

- ISO/IEC 9594-8:2001 "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certification Frameworks" as well as

- ISO/IEC 8802-11:2005 "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".

AFNOR strongly requests that these contradictions be resolved by ITTF and JTC 1 Secretariat in accordance with JTC 1 Procedures clause 13.2 before ballot voting commences.

Kind regards,

Tony HITTEMA
AFNOR - DTEC
Tél. : +33 1 41 62 83 95 / Fax : +33 1 49 17 90 33 http://www.afnor.fr

Schweizerische Normen-Vereinigung
Association Suisse de Normalisation
Swiss Association for Standardization

To the attention of:

Secretariat JTC 1 - Mrs Lisa Rajchel
ITTF - Mr. Keith Brannon

PER E-MAIL

Winterthur, 2005-10-04

Edith Hugentobler
edith.hugentobler@snv.ch
Tel. +41 (0)52 224 54 18
Fax +41 (0)52 224 54 74

Contradictions observed during the review period of Amendment 7 to ISO/IEC 8802-11:2005 as given in ISO/IEC JTC 1 N7904

Ladies and Gentlemen

The Swiss National Body to ISO/IEC JTC 1 wants to express two types of contradictions with respect to draft Amendment 7 to ISO/IEC 8802-11:2005 submitted for adoption under the fast-track procedure:

A. Procedural

B. Concerning the contents of Draft Amendment 7 to ISO/IEC 8802-11:2005.

A. Procedural issues

We have received a letter on this subject from the Secretaries General of ISO and IEC, dated 2005-09-06, i.e. at the beginning of the review period concerned. This letter states, in the third paragraph, that …. *irrespective of the result of the review period, both proposals will now be submitted for parallel fast-track ballot on 07 October 2005* ….

This is an obvious contradiction to the JTC 1 Directives that state in 13.4:

During the 30-day review period, an NB may identify to the JTC 1 Secretariat any perceived contradiction with other JTC 1, ISO or IEC standards.

If such a contradiction is alleged, the matter shall be resolved by the ITTF and JTC 1 Secretariat in accordance with Section 13.2 before ballot voting can commence. If no contradiction is alleged, the fast-track ballot voting commences immediately following the 30-day period.

The Swiss NB requests that the JTC 1 Directives are fully and correctly applied. We would highly appreciate a revised letter that precisely states this. If these Directives are not correctly applied, the Swiss NB will have to vote NO, if only for procedural reasons.

We also use this opportunity to express our concerns about several inaccuracies in N7904, such as:

- 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.
- The existing standard is not a DIS but the unanimously approved second edition of ISO/IEC 8802-11 published in 2005.

B. Concerning the contents of Draft Amendment 7 to ISO/IEC 8802-11:2005.

A basic requirement for an Amendment is that it has to dovetail into the standard to be amended. Draft Amendment 7 does not satisfy this requirement. To the contrary, it breaks ISO/IEC 8802-11 on several occasions, and is even partially out of the scope of this standard.
Additionally, there is a contradiction with ISO/IEC 9594.

The following information provides detailed reasons for these grave contradictions:

1. Clause 8 of N7904 deletes the – deprecated - security mechanism called WEP (Wired Equivalent Privacy) and defines a new mechanism called TKIP (Temporal Key Integrity Protocol). However, WEP has to be retained if only for legacy reasons. Many millions of devices will no longer comply with the standard if WEP is removed: it also does not harm anybody if WEP is retained. TKIP is not a viable solution either because these devices cannot support the more advanced cipher suites of TKIP.
2. Sub-clause 8.1.4.2 is beyond the scope of ISO/IEC 8802-11, i.e. beyond the WLAN (Wireless Local Area Network) technology. The sub-clause proposes to include all aspects of WAI (WAPI Authentication Infrastructure, where WAPI stands for Wireless LAN Authentication and Privacy Infrastructure) into a standard that only specifies Layers 1 and 2, i.e., MAC (Medium Access Control) and PHY (Physical Layer). The WAI authentication scheme is not only outside the scope of the standard but also outside the programme of work of its originator JTC 1/SC6: probably JTC 1/SC27 would be the most suitable SC to deal with this subject. An authentication scheme should not be limited to a (W)LAN but serves a much broader audience.
3. Sub-clause 8.1.3 contradicts ISO/IEC 9594 that specifies a standard digital certification format. This is a subject of interest to JTC 1/SC6 and the ITU. N7904 defines a new digital certification format and, therefore, belongs in ISO/IEC 9594, if at all.
4. The development of ISO/IEC 8802-11 has cost over 200 man-years and has been developed following several rules and proven practices laid down in ISO/IEC 8802-1:2001. N7904 is completely bypassing this approach, not only in terms of process but also in terms of good engineering. For example, it 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. Moreover, if accepted, it would soon be ‘cracked’ by hackers, which only puts the method in a bad light.

As a final remark, we would like to make the observation that there is a lot of interest in the WAPI technology, in particular also in JTC 1/SC6. It would be a pity if the WAPI technology could not be standardised in an appropriate way. A special meeting on the subject held in Beijing on 8-12 August 2005 has identified and explored two viable ways forward to standardise WAPI. It would be regretful if this could not lead to an international result.

We do not believe that the contradictions mentioned above can be resolved in a very short time period, e.g., three months. Therefore, we do not believe that fast-track processing is a suitable way forward to bring the WAPI technology to international standards level: there are better, and viable, ways to do that. The time spent on fast-track processing of Draft Amendment 7 is a waist of time.

Schweizerische Normen-Vereinigung
Association Suisse de Normalisation
Swiss Association for Standardization

Even if the document is accepted, with or without violation of the JTC 1 Directives, the international standardisation community would not find an easy way to dovetail (parts of) the Amendment into ISO/IEC 8802-11:2005.

Concluding, it is very likely that the Swiss NB has to vote NO to the proposal if it progresses to a fast-track ballot vote.

Yours faithfully

SNV Swiss Association for Standardization

Edith Hugentobler

Annex: Letter from Secretaries General of ISO and IEC 2005-09-06

Tecnologie informatiche e loro applicazioni

UNINFO

Ente di normazione federato all'UNI

Corso G. Ferraris, 93 - 10128 Torino - Italia
tel. + 39 011 501027 - fax + 39 011 501837
cod. fisc. 80082520018 - p.iva 06476530016
e-mail: uninfo@uninfo.polito.it - http://www.uninfo.polito.it

Turin, 2005-10-06

Italian comments on document ISO/IEC JTC1 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) "

Contradictions

1)
In accordance with JTC 1 procedures, clause 13.4 on 30 day review period during fast-track, we have identified contradictions between doc. JTC1 N 7904 and existing ISO/IEC standards.

a) The doc. JTC1 N 7904 contradicts ISO/IEC 9594-8, "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certification Frameworks".

2) The doc. JTC1 N 7904 proposal is in contradiction with ISO/IEC 8802-11 as it does not, allow backword compatibility, among others, for WEP.

3) We requests that these contradictions be resolved by ITTF and JTC 1 Secretariat in accordance with JTC 1 Procedures clause 13.2 before ballot voting commences.

Procedural comments:

The ballot period should not start before the resolution of all the contradictions with ISO/IEC existing standards.

Date
2005-10-06

Reference
J1N7904

Handled by, phone
Susanne Björkander, 08-555 524 93
E-mail
susanne.bjorkander@sis.se

SE comments on Fast Track Ballot for Draft Amendment ISO/IEC DIS 8802-11/Amd.7 (JTC1 N 7904)

SIS Steering committee for IT Standardization (SIS/TK 447) has in review of JTC1 N 7904 found contradictions between the N 7904 and the existing ISO/IEC 9594-8.

SIS Steering committee for IT Standardization (SIS/TK 447) requests that the contradictions identified need to be resolved by ITTF and JTC1 Secretariat. This should be done in accordance with the JTC1 procedures in clause 13.2 before voting starts.

ISO/IEC 9594-8: "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certification Frameworks"

SIS, Swedish Standards Institute
SIS is the Swedish member of ISO and CEN

Postadress: 118 80 STOCKHOLM
Telefon: 08-555 520 00 Telefax: 08-555 520 01
Besöksadress: Sankt Paulsgatan 6, Stockholm
E-post: info@sis.se
Organisationsnr: 8024100151

Postal address: SE-118 80 STOCKHOLM, Sweden
Phone: +46 8 555 520 00 Telefax: +46 8 555 520 01
Office address: Sankt Paulsgatan 6, Stockholm
E-mail: info@sis.se
V.A.T. No. SE802410015101
www.sis.se

From: David Keech [David.Keech@BSI-GLOBAL.COM]
Sent: Thursday, October 06, 2005 6:01 AM
To: Lisa Rajchel
Cc: r.tasker@dl.ac.uk; Trevor Vyze; Adrian.Stokes@cat-ltd.demon.co.uk; bob.carter@ukonline.co.uk; dave_sawdon@uk.ibm.com; David Keech; francis@franciscave.com; GEOFF.SMITH@DTI.GSI.GOV.UK; jack.cogman@thales-tts.com; james.whittle@apacs.org.uk; jon.diamond@btinternet.com; nine_tiles@psilink.co.uk; schemeta@mac.com; Mike Graham; paul.a.jenkins@bt.com; MD@PENTAD.CO.UK; Peter.Gibbon@open-it.co.uk; pr_brown@compuserve.com; ray765_4rogers@ntlworld.com; richard.rees@virgin.net; Richard Taylor; Rob Anderson; ROBWALKER@CIX.CO.UK; roy.reed@sun.com; tedxisecltd@aol.com; verina.horsnell@dial.pipex.com
Subject: UK response on J1N7904 30 Day Review for Fast Track Ballot for Draft Amendment ISO/IEC DIS 8802-11/Amd.7

Dear Lisa

The UK wishes to submit the following comment on this 30 Day Fast Track Ballot review (deadline 7 October 2005).

The UK welcomes the letter from the Secretaries General of ISO and IEC dated 6 September 2005 announcing the start of the fast-track processing of IEEE 802.11i and SAC's WAPI proposal and endorses the use of the JTC1 fast-track procedure in this instance including a 30-day National Body review and comment period. The UK notes that this is "...on the understanding that, irrespective of the result of the review period, both proposals will now be submitted for parallel fast-track ballot on 7 October 2005..." and that "...both will close simultaneously and the results addressed in a joint ballot resolution meeting...".

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.

Furthermore, we consider that the mark-up format in J1N7904 is unsuitable for publication as an amendment to an International Standard.

The proposed changes in J1N7904 constitute a contradiction to the current International Standard, ISO/IEC 8802-11:2005 which is technical equivalent to IEEE 802.11 which had been through a rigorous development and approval process in the IEEE before being adopted by JTC 1 as a fast-track standard.

The UK notes the exceptional procedures that the Secretaries General of ISO and IEC have agreed and expect that the procedures being used in this case will not create a precedent

US National Body Comments in Response to 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)

1 Summary

This document identifies “contradictions” between JTC 1 N 7904 (“WAPI”) and existing ISO/IEC standards and processes.

The scope of these contradictions suggests that the fast track ballot on JTC 1 N 7904 should not enter the 5 month balloting stage of the balloting process.

The contradictions are:

1. JTC 1 N 7904 Clause 8.1.3 contradicts ISO/IEC IS 9594.
2. JTC 1 N 7904 Clause 8.1.4.2 is outside the scope of ISO/IEC IS 8802-11:2005
3. JTC 1 N 7904 Clause 8 contradicts clause 8.2 of ISO/IEC IS 8802-11:2005
4. JTC 1 N 7904 was developed using a process contradicting ISO/IEC TR 8802-1:2001

2 JTC 1 N 7904 Clause 8.1.3 contradicts ISO/IEC IS 9594

ISO/IEC IS 9594 defines a standard digital certificate format. It was co-developed by ITU-T and JTC1/SC6/WG7.

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 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.

JTC 1 N 7904 must not enter the 5 month balloting stage until clause 8.1.3 is removed. The material in clause 8.1.3 should be referred to JTC1/SC6/WG7 or some other appropriate forum.

3 JTC 1 N 7904 Clause 8.1.4.2 is beyond the scope of ISO/IEC IS 8802-11

ISO/IEC IS 8802-11 standardizes layer 1 and layer 2 WLAN technologies.

JTC 1 N 7904 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.
JTC 1 N 7904 must not enter the 5 month balloting stage until clause 8.1.4.2 is removed. The material in clause 8.1.4.2 should be referred to JTC1/SC27 or some other appropriate forum. This should be done as soon as possible because the authentication scheme will have value in many user environments.

4 JTC 1 N 7904 clause 8 contradicts ISO/IEC IS 8802-11 clause 8.2

ISO/IEC IS 8802-11 includes an insufficient security mechanism called WEP. Over 200 million deployed WEP-only devices conform to ISO/IEC IS 8802-11:2005.

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.

JTC 1 N 7904 should not enter the 5 month balloting stage until WEP devices are supported. Support could follow the example of JTC 1 N 7903, which deprecates rather than deleting WEP and defines an upgrade path called TKIP (see JTC 1 N 7903 clause 8.3.2) for devices that cannot use more advanced cipher suites.

5 JTC 1 N 7904 contradicts 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.

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”.

Strictly speaking, this is not a contradiction, since the review period is meant only to identify contradictions with international standards, not with technical reports. However, pointing out that no attempt was made to adhere to the established procedures used to co-develop IS 8802-11 is relevant in understanding why JTC 1 N 7904 includes contradictions. JTC 1 N 7904 should not enter the 5 month balloting stage until at least the spirit of ISO/IEC TR 8802-11:2001 is fulfilled.

Australian response to JTC1 N7904

Fast track review of:

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)

Summary

The Australian National Body has identified the following contradictions with existing ISO/IEC standards and the proposal contained in JTC1 N7904 ("WAPI").

We believe that these contradictions should be resolved prior to the proposal being submitted to a fast track DIS ballot.

The contradictions are:

1. JTC1 N7904 Clause 8.1.3 contradicts ISO/IEC 9594 Information technology - Open Systems Interconnection - The Directory series.
2. JTC1 N7904 Clause 8.1.4.2 is outside the scope of ISO/IEC IS 8802-11:2005 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
3. JTC1 N7904 Clause 8 contradicts clause 8.2 of ISO/IEC IS 8802-11:2005 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
4. JTC1 N7904 was developed using a process contradicting ISO/IEC TR 8802-1:2001 Information technology - Telecommunications and information exchange between systems -- Local and metropolitan area networks - Specific requirements - Part 1: Overview of Local Area Network Standards

1 JTC1 N7904 Clause 8.1.3 contradicts ISO/IEC IS 9594

ISO/IEC 9594 Information technology - Open Systems Interconnection - The Directory defines a standard digital certificate format. It was co-developed by ITU-T and JTC1/SC6/WG7.

JTC1 N7904 defines a new digital certificate format in clause 8.1.3. However, given ISO/IEC 9594 governs certificate formats, this topic is out of scope for an amendment to ISO/IEC IS 8802-11. JTC1 N7904 does not justify its deviation from ISO/IEC 9594.

2 JTC1 N7904 Clause 8.1.4.2 is beyond the scope of ISO/IEC IS 8802-11

ISO/IEC 8802-11 standardizes layer 1 and layer 2 WLAN technologies.

JTC1 N7904 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.

3 JTC1 N7904 clause 8 contradicts ISO/IEC IS 8802-11 clause 8.2

Over 200 million deployed WEP-only devices conform to ISO/IEC 8802-11:2005.

JTC1 N7904 clause 8 contradicts ISO/IEC 8802-11:2005 clause 8.2 by deleting the definition of WEP. Adoption of JTC1 N7904 would instantly render every one of the existing WEP devices non-conformant, which is clearly undesirable for an international standard.

4 JTC1 N7904 contradicts 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.

We are concerned that JTC1 N7904 may have been developed without “rigorous technical appraisal” by all stakeholders, including ISO/IEC NBs and IEEE 802, and that this may be in contradiction to the process outlined in TR 8802-11:2001.

Title: **Japanese comments on JTC1N7904, 30 Day Review for Fast Track Ballot for Draft Amendment ISO/IEC DIS 8802-11/Amd.7**

Source: **The national body of Japan**

Japan points out the following “contradictions” between JTC 1 N 7904 (“WAPI”) and the existing ISO/IEC standards:

1. JTC 1 N 7904 contradicts ISO/IEC 8802-11:2005, because the definition of WEP is not included.

2. JTC 1 N 7904 contradicts ISO/IEC 9594-8, because a new digital certificate type is included as an alternative to the one specified in the ISO/IEC 9594-8.

In addition, the specification of the cryptographic technology “SMS4” included in JTC 1 N 7904 is not clear.

JTC 1 N 7904 must not enter the 5 month balloting stage until the above contradictions and immaturity are resolved according to the JTC 1 Directives section 13.4.

Amsterdam, October 11, 2005

Subject: Observer contribution in relation to the Draft Amendment ISO/IEC DIS 8802-11/Amd.7

Based on the Observing Membership for ISO/IEC JTC1/SC 6 of the Netherlands, this document represents the Dutch contribution in relation to the Fast Track Ballot corresponded by document ISO/IEC JTC1 N7904.

This Observer contribution is based on the vision of interested Dutch market parties. The wireless LAN industry is very concerned that a positive vote result could lead to 80211i based equipment being excluded from the Chinese market.

Short Summary

Hereby receive you a short summary of our concerns in relation to the two wireless LAN security standards now being put out for a vote under the fast track procedure by ISO/JTC1. One of these is the IEEE 802.11i standard; the other is the Chinese national standard for wireless LAN security 1N7904, known as "WAPI".

As is frequently the case with issues like these, the history that led to the current situation of two standards that cover the roughly same ground but being fast tracked in parallel, is quite complex and in some ways unfortunate. The key elements of that history are captured in the annexed paper (Gao). It also gives some insight into the internal political landscape of the Chinese government.

Clearly, the preferable way forward is a harmonization of two standards and the IEEE 802.11 Working Group has made every effort to work together with the Chinese proponents of WAPI. These efforts have stranded on Chinese unwillingness to work together on the basis of harmonisation procedures agreed by ISO and the IEEE. See 8802-1:2001 (Feb 01).

The broad reasons of the international wireless LAN industry – as represented in the IEEE 802.11 Working Group – for advising National Bodies NOT to vote YES on the Chinese WAPI standard are laid out *in extenso* in the enclosed presentation. In addition, IEEE technical experts are developing a comprehensive, technical set of comments on the WAPI standard. These provide a technical basis for voting NO on the WAPI standard.

There are other considerations: 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. That this threat is real, is demonstrated by the fact that in 2001, the Chinese government already announced such a border closure in late 2003.

Nederlands Normalisatie-instituut
Vlinderweg 6, 2623 AX Delft, NL – Postbus 5059, 2600 GB Delft, NL
Telefoon +31 (0)15 2 690 390, Fax +31 (0)15 2 690 190, Internet: www.nen.nl

To quote the attached paper:

"On November 26th, 2003, AQSIQ with SAC issued Decree Number 110, which announced that from 1st December, it was prohibited to produce, import and sell WLAN products that did not comply with WAPI standard. Five day later, AQSIQ and National Regulatory Commission for Certification and Accreditation issued Decree Number 113. This decree extended the compliance deadline for some WLAN products until June 1st, 2004. As a result, China has refused to adopt Wi-Fi, because this popular standard needed technological improvement for better information security (Pan and Fu, 2004).
The corresponding problem with WAPI was that it was a proprietary protocol controlled by the Chinese government. BWIPS alleged that, by "Business Encryption Management Regulation", which was published as Decree Number 273 by the State Council in October 1999, the WAPI algorithm was a national secret and hence could only be authorized to specific Chinese companies. 11 Chinese companies, including Lenovo and Huawei, were [designated] by the Chinese government to have the algorithm. Foreign equipment vendors that wanted to sell WLAN products in China were required to license WAPI through a manufacturing agreement with one of these Chinese companies (Chen, 2003)."

That policy was not enforced – under pressure, China agreed to:

"1. suspend indefinitely its proposed implementation of WAPI as a mandatory wireless encryption standard;
2. work to revise its WAPI standard, taking into account comments received from Chinese and foreign firms;
3. participate in international standards bodies on WAPI and wireless encryption for computer networks.

That process is still ongoing and the result is the current "two fast tracks vote".

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; however, those "contradictions" in WAPI could not be resolved before the five-month ballot starts. In a letter dated September 6, 2005, the Secretary-General of ISO stated that, "…irrespective of the results of the review period, both proposals will be submitted for fast-track ballot on 07 October 2005…". This procedure is remarkable to say the least.

There are obvious concerns that approval of the WAPI standard under these circumstances would set a precedent with broad negative implications across a wide spectrum of technical standards.

Finally, 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.

"Contradictions" between 1N7904 ("WAPI") and existing ISO/IEC standards and processes

Summary

This document identifies "contradictions" between 1N9704 ("WAPI") and existing ISO/IEC standards and processes.
The scope of these contradictions suggests that the fast track ballot on 1N9704 should not enter the 5 month balloting stage of the balloting process.
The contradictions are:

1. 1N7904 Clause 8.1.3 contradicts ISO/IEC IS 9594.
2. 1N7904 Clause 8.1.4.2 is outside the scope of ISO/IEC IS 8802-11:2005
3. 1N7904 Clause 8 contradicts clause 8.2 of ISO/IEC IS 8802-11:2005
4. 1N7904 was developed using a process contradicting ISO/IEC TR 8802-1:2001

1N7904 Clause 8.1.3 contradicts ISO/IEC IS 9594

ISO/IEC IS 9594 defines a standard digital certificate format. It was co-developed by ITU-T and JTC1/SC6/WG7.
1N7904 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.
1N7904 does not justify its deviation from ISO/IEC IS 9594
The material in clause 8.1.3 should be referred to JTC1/SC6/WG7 or some other appropriate forum.

1N7904 Clause 8.1.4.2 is beyond the scope of ISO/IEC IS 8802-11

ISO/IEC IS 8802-11 standardizes layer 1 and layer 2 WLAN technologies.
1N7904 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.
IN9704 must not enter the 5 month balloting stage until clause 8.1.4.2 is removed. The material in clause 8.1.4.2 should be referred to JTC1/SC27 or some other appropriate forum. This should be done as soon as possible because the authentication scheme will have value in many user environments.

1N7904 clause 8 contradicts ISO/IEC IS 8802-11 clause 8.2

ISO/IEC IS 8802-11 includes a discredited security mechanism called WAPI. Over 200 million deployed WEP-only devices conform to ISO/IEC IS 8802-11:2005.
1N7904 clause 8 contradicts ISO/IEC 8802-11:2005 clause 8.2 by deleting the definition of WEP. Adoption of 1N7904 would instantly render every one of the over existing WAPI device as non-conformant, which is clearly 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.

1N7904 contradicts 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.
However, 1N7904 was developed independently and without any coordination with the community developing ISO/IEC IS 8802-11 and its amendments, thus avoiding the necessary “rigorous technical appraisal”.

From: Nelson Procter [mailto:Nelson.Procter@standards.co.nz]
Sent: Monday, October 10, 2005 8:34 PM
To: lrajchel@ansi.org
Subject: Fwd: RE: Australian response to JTC1 N7904

Dear Lisa,

New Zealand cannot support N7904 proposals and wishes to support the Australian position attached.

We support the ongoing development of this technology within the IEEE environment and see it as very necessary that the WAPI supporters be encouraged in every way possible to meet together with the IEEE group and make every endeavour to constructively work together towards a consensus solution.

Best wishes,

Nelson Procter
ISO Administrator
Standards NZ

From: NIKOLAUS KOVACS [NIKOLAUS.KOVACS@DIN.DE]
Sent: Friday, October 07, 2005 5:42 AM
To: lrajchel@ansi.org
Cc: michael_breidthardt@de.ibm.com
Subject: Germany on Review period of Amendment 7 to ISO/IEC 8802-11:2005

Subject: Review period of Amendment 7 to ISO/IEC 8802-11:2005 as given in ISO/IEC JTC 1 N7904

Dear Lisa!

In a letter dated 2005-09-06 from the Secretaries General of ISO and IEC on this subject the third paragraph states that .... "irrespective of the result of the review period, both proposals will now be submitted for parallel Fast-track ballot on 07 October 2005 ...."

This is an obvious contradiction to the JTC 1 Directives that state in 13.4:

"During the 30-day review period, an NB may identify to the JTC 1 Secretariat any perceived contradiction with other JTC 1, ISO or IEC standards. If such a contradiction is alleged, the matter shall be resolved by the ITTF and JTC 1 Secretariat in accordance with Section 13.2 before ballot voting can commence. If no contradiction is alleged, the fasttrack ballot voting commences immediately following the 30-day period."

The German NB would like to point out that such contradictions in our opinion do exist (see below) and therefore asks that the JTC 1 Directives are correctly applied and any contradiction be resolved before the fasttrack voting commences.

Such contradictions are:

1N7904 Clause 8 contradicts clause 8.2 of ISO/IEC IS 8802-11:2005

1N7904 Clause 8.1.3 contradicts ISO/IEC IS 9594-8 "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certification Frameworks"

1N7904 Clause 8.1.4.2 is outside the scope of ISO/IEC IS 8802-11:2005

Best regards,

Nikolaus