中国对有关 1N7904 评论的回应

中国国家成员体

2005 年 11 月 30 日

以下是中国国家成员体直接对ISO/IEC JTC1所有国家成员体的通信，用于解释 JTC1 文件“**国家成员体对JTC 1N 7904的评论汇编，ISO/IEC DIS 8802-11/Amd.7快速程序投票30天评论期内的评论，信息技术—系统间远程通信和信息交换—局域网和城域网—特定要求—第11部分：无线局域网媒体访问控制（MAC）和物理层（PHY）规范—修正案7：增强性安全规范—WLAN鉴别与保密基础结构（WAPI）**”中相关的问题和评论。

本文档同时发送给了ISO/IEC中央秘书处、JTC1秘书处、以及其他有关团体以供参考。由于本文档涉及的提案进入了投票阶段，因此不允许在投票期内进行官方讨论。本文档将作为中国国家成员体与各个相关团体之间的直接通信。

1. 评论需要立即解决

根据 2005 年 5 月 17 日于日内瓦 ISO 总部召开的 ISO/IEC 特别工作组会议的决议，中国国家成员体向 ITTF 重新提交了 WAPI 提案以便在 2005 年 9 月 7 日开始快速程序投票。2005 年 9 月 6 日，ISO 秘书长 Alan Bryden 与 IEC 秘书长 Aharon Amit 发布了一个决定：IEEE

802.11i 和 WAPI 提案同时开始快速流程，并且无论一个月评论期内的评论结果如何，两个提案都将在 10 月 7 日进入五个月的投票期，并同时（也就是 2006 年 3 月 7 日）投票结束。WAPI 提案被给予了新的文件号 1N7904，并且在 10 月 7 日，与 11i (目前文件号 1N7903) 一同进入 40.20 投票阶段。然而，中国国家成员体注意到在进入投票阶段之前，11 个国家成员体对 1N7904 进行了评论或观察报告。

中国国家成员体始终欢迎评论，并且在过去的一年里，我们为了接纳各种评论和解决关于 WAPI 的担心，已经做出了巨大努力。虽然 WAPI 已经进入了非评论期，并且这些评论可以在投票分析阶段进行解决，但我们认为这些评论不可以在目前这个阶段被忽视，所做的解释不可以被延迟。我们已经注意到某些国家成员体评论说如果他们提出的问题不被解决，他们将投票反对 WAPI。

因此，中国国家成员体必须对这些评论做出回应。可是，我们正处于两个提案都进入了非评论期的棘手局面中，并且在投票结束以前，(ISO)没有要召开技术会议的计划。唯一可行的方法就是中国国家成员体积极地、善意地与提交评论的国家成员体进行非正式的交流。但这可能会使那些没有提交评论的国家成员体只能看到其他国家成员体的评论而看不到中国国家成员体关于这些评论的解释，这将限制我们解释的效力，并有可能削弱对 WAPI 的支持。

所以，一个全面概括性的评论解决方案（解释）是有必要的，并应发送给 JTC1 和 SC6 内的所有国家成员体。

2. 评论概要

所有评论可以被归纳为 10 个问题：

#1) WAPI与其它标准相冲突。这些冲突应当由ITTF和JTC1秘书处按照JTC1程序条款13.2，在投票开始以前予以解决。

#2) 1N7904 (WAPI)不是一个国际标准草案的快速流程提案，而是对现有标准修订的草案。因此，ITTF 的注解（说 WAPI 是国际标准提案）着实让人糊涂。

#3) JTC1 导则规定快速流程适用于没有修改过的现有的标准（可以是任何来源）。1N7904 中的文字与中国国家标准 GB15629.11-2003 以及中国上一次的提案 SC 6N12687 有明显的改动，因此它不符合快速流程的条件。

#4) 1N7904 (WAPI) 条款8.1.3与ISO/IEC IS 9594-8:2001相矛盾。它定义了一种新的数字证书格式，可是证书格式问题由ISO/IEC IS 9594管理，这个问题超出了ISO/IEC IS 8802-11补篇的范围，1N7904没有证明它违背 ISO/IEC IS 9594是正当的。

#5) 1N7904 (WAPI) 条款 8.1.4.2 超出了ISO/IEC IS 8802-11:2005的范畴。它定义了一种新的鉴别机制，但鉴别机制问题超出了ISO/IEC 8802-11补篇的范围。

#6) 1N7904 (WAPI) 条款8与ISO/IEC IS 8802-11:2005条款8.2相矛盾。它删除了WEP的定义。如果采用1N7904，将立即导致每一个现有的只支持WEP的设备不被兼容，对于一个国际标准来说，这是不受欢迎的。

#7) 1N7904 (WAPI)的开发过程与ISO/IEC TR 8802-1:2001相矛盾。ISO/IEC TR 8802-11:2001指定了JTC1/SC6/WG1与IEEE 802的协作关系，以保证有关各方可以进行“严格的技术鉴定”，包括ISO/IEC国家成员体和IEEE 802。

#8) 1N7904 (WAPI) 定义了一种新的加密方法，但却没有提供任何有关设计上或强健性上的细节。这已经被证明是局域网方面一种很糟糕的处理方法，无法给人以高可靠性的印象。

#9) 如果 WAPI 成为国际标准，中国将决定对非 WAPI 兼容的 WLAN 产品关闭大门，而中国的制造厂商在从中国出口时将不会面临这种限制。

#10) 中国的WAPI支持者已经赢得了中国国家成员体的支持，但是有证据表明这个组织并没有获得中国部级领导层的支持。因此不支持WAPI标准不会必然地伤害与中国领导层的关系。

3. 国家成员体及其所提出的问题

国家 / 意见	美国	英国	法国	德国	日本	荷兰	意大利	瑞士	瑞典	新西兰	澳大利亚
违反程序规则		●	●	●		●	●	●	●		
是标准的补篇而不是标准								●			
不是已存在的标准		●									
违反了 ISO 与 IEEE 的合作	●					●				●	●
定义了新的证书格式	●		●	●	●	●	●	●	●	●	●

WAI 超出范围	●			●		●		●		●	●
删除了 WEP	●	●	●	●	●	●	●	●		●	●
加密算法 不公开					●			●			
设置贸易壁垒						●					
未获国家高级 领导层支持						●					

4. 概括性观点

中国国家成员体仔细研究了所有的评论，发现绝大多数所提出的问题在以前多次的相关国际会议中就已经被提出，并且中国国家成员体在这些会议上已经出示了大量的细节性文件来解释和解决这些问题。只有问题#2 和#10 是新的问题。问题#2 是一个 ITTF 公告中不准确的描述。问题#10 实际上不是一个（在评论期内）恰当的论题，不应该作为考虑的要素。

不过，为了消除任何存在的担心并证明 WAPI 作为国际标准的资格与实力，我们将在本文档中再一次系统地回答这些问题。我们希望我们的努力能够令各国家成员体满意，并希望能够赢得他们对 WAPI 的支持。

5. 针对问题的详细解答

问题 #1：违反程序规则

某些评论说：*“ISO/IEC JTC1 导则要求投票成员必须审核和评论文档，任何与 ISO 或 IEC 标准冲突的地方必须在投票之前解决。WAPI*

与其它标准有很多周知的“冲突”，在投票开始之前，ITTF 和 JTC1 秘书处应当根据 JTC1 程序的条款 13.2 解决上述冲突。”

中方的回应:

以下几个方面需要被考虑：

1) 这个顾虑已经被解决

这个问题在 SC6 2005 年法国年会（8 月 29 日-9 月 2 日，法国 St. Paul De Vance）上已经被提出，中国国家成员体也已经在法国会议上用以下具体文件做出了回应：“SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status”与 6N12960 “notes from Chinese national body” (2005 年 8 月 31 日).

2) WAPI 已经接受了长期的评论

从 2004 年 8 月 2 日到 2005 年 9 月 6 日，WAPI 已经经历了一个极其长的、乃至扩大范围的评论期。这个评论期（共 13 个月）已经大大超出了快速流程所需要的一个月以及 NP 流程所需要的 2-3 个月。

3) 各国家成员体有很多的机会和很长的周期来研究 WAPI 提案并进行评论.

在此期间：

- 2004 年 8 月 2 日，WAPI（1N7506）传发给各国家成员体进行为期三个月的评论；
- 2004 年 8 月 25 和 26 日，收到了关于 WAPI 的评论（6N12713、6N12712）；
- 2005 年 7 月, WAPI 提案(WAPI N 16) 由 ISO/IEC 中央秘书处

分发给各国家成员体，并在 ISO/IEC 网站上公布，供公众访问、评论；

- 2005 年 8 月，WAPI 重新提交给 ITTF 进行快速程序投票。

4) 评论已在五次国际会议中得到解决

在长达一年多的评论期内, WAPI 收到了许多评论，这些评论得到了高度的关注。

这些评论在以下会议中得到了圆满的解决：

- 2004 年 11 月 8-12 日, 美国奥兰多，SC6 2004 全会
- 2005 年 2 月 21-23 日, 德国法兰克福，SC6/WG1 特别会议
- 2005 年 5 月 17 日, 瑞士日内瓦，ISO/IEC 特别工作组会议
- 2005 年 8 月 8-12 日, 中国北京，ISO/IEC 特别工作组会议
- 2005 年 8 月 31 日-9 月 2 日, 法国 St. Paul De Vance，SC6 2005 全会

5) 这些会议的结果

- 在 SC6 奥兰多会议上, 讨论了 WAPI 的快速程序资格问题，并得出了肯定的结论。
- 在奥兰多会议上, IEEE 宣布：“WAPI 与 11i 不是互斥排他性的，它们可以并存于 ISO/IEC 8802-11 中并在需要的时候被调用。”（6N12768，IEEE 代表团评论文件）
- 在奥兰多会议上, 决议允许 WAPI 和 11i “同时在 SC6 中独立推进。”（6N12765，SC6 奥兰多会议文件）
- 2005 年 1 月, JTC1 秘书处裁定 WAPI 已经完成了一个月的评

论期，可以进入投票阶段。（ISO/IEC JTC1 秘书处 Lisa Rajchel 写给中国国家成员体的信件，2005 年 1 月 28 日）

- 在日内瓦会议上，以无异议协商一致原则下所通过的最后决议批准 WAPI 于 2005 年 9 月 6 日开始投票，英国、美国以及 IEEE 的代表均同意这一决议。
- 在北京会议上，有关文件再次表明，两个提案不是互斥排他性的，他们可以以可选的方式并存于 ISO/IEC 8802-11 中并在需要的时候被调用。
- 2005 年 9 月，ISO/IEC 中央秘书处做出了合理的、考虑周到的决定：2005 年 10 月 7 日，WAPI 和 11i 同时进入快速流程投票。（参见日内瓦会议决议“Resolutions from the special work group meeting_Geneva_May 17_2005”）

6) 我们遵守规则

有一种观点认为中国国家成员体把 WAPI 推进到投票阶段，没有遵守有关规定和常规程序，我们强烈反对这一观点。

中国国家成员体详细地研究了有关规则和程序，并且严格地遵守。中国国家成员体没有任何违反规定和导则的行为。

我们必须指出，是一系列不公正的待遇和其他组织对规则的违反，导致 ISO/IEC 中央秘书处召集了日内瓦特别会议。在那次会议上，在听取了所有事实和争论以后，经与会各方一致同意决定继续延缓 11i 的投票，并一致同意在 9 月 6 日开始 WAPI 和 11i 的共同进行的快速流程投票。任何对这一决定的修改，应再次通过参加那一次会议

的有关各方一致同意。

结论:

WAPI 与 11i 提案的冲突已经在 2004 年 8 月的评论期内被提出来，并且已经在随后的一系列国际会议中被圆满地解决了。这些会议包括：奥兰多 SC6 2004 全会、法兰克福 WG1 特别会议、日内瓦 ISO/IEC 特别工作组会议、北京特别会议、法国 SC6 2005 全会(St. Paul De Vance)。冲突已经被解决，一系列的决议已经批准 WAPI 进入投票阶段。这些决议反映出了这样一种决心：所谓的“冲突”不应该阻止 WAPI 或 11i 在 10 月 7 日进入投票，并且不应该以此为理由反对 WAPI。WAPI 在十月份进入投票阶段，是一个合情合理的、共同协商一致的、积极的决定。

问题 #2：是标准的补篇而不是标准

某些评论说:“*这不是对标准草案的快速程序投票，而是对现存标准的修正案草案。因此，ITTF 中第3页的注释很令人费解。*”

中方的回应:

WAPI 和 11i 都是 ISO/IEC 8802-11 的增强安全的补篇提案。它们不是互斥排他性的，它们可以以可选的方式并存于 ISO/IEC 8802-11 中并在需要的时候被调用。

问题 #3: 不是已存在的标准，文字上有改动

某些评论说：“*JTC 1 导则指出快速程序仅仅适用于未经修改而提*

交的（来自任何来源的）已存在的标准。J1N7904 的文档与中国标准 2003 年的 GB15629.11 相比有显著的修改，与中国提交的 SC6 N12687 也有显著差别。除非可以证明 N7904 的文档在提交之时与已经发布的中国标准完全相同，否则进行快速程序就是不恰当的。”

中方的回应:

1) 这是一个老问题了，这个问题已经由 IEEE 代表团在 ISO/IEC 北京会议上提出。

2) 我们之前已经解释过了，对这个问题的回答就在由中国代表团在法国 SC6 2005 全会（St. Paul De Vance）上提交的一份文件中，题目是“SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status”。其中，中国国家成员体进行了以下解释：

“为什么要改动?

有一种观点认为 WAPI 提案改动了好几次，这表示它并不成熟。

中国国家成员体希望提请注意以下几点事实：

- *WAPI 是一种成熟的技术，已经成为中国的国家标准。*
- *所有的改动都是微小的，主要是为了使 WAPI 更适合国际标准的要求。*
- *WAPI 结构的整体性没有被改变，其安全机制的强度也没有被削弱。*
- *在快速流程投票前作适当的改动，是ISO/IEC 导则所允许的。”*

3) 快速程序并不阻碍评论和建议。

JTC1 导则规定（JTC1 导则，第五版，第 55 页）:

“在提交快速程序文件之前，JTC1 的P 成员或A 类联络组织可以申请通过JTC1 秘书处向一个或多个分委员会提交该文件以便在有兴趣的团体间进行非正式评论或讨论。有关格式，技术内容，完整性等任何评论意见均可由申请者在正式提交该文件进行快速程序处理之前予以考虑。”

4) 改动并不违反快速程序

程序规则并不阻止在投票开始前进行改动，投票开始以后，改动才是被禁止的。

JTC1 导则规定（JTC1 导则，第五版，第 62 页）：

“M.7.3.1.3　转换过程中的改动

提案人在转换过程中对规范进行技术或编辑上的修改，其目的是什么?

认可的PAS 提交人可以在转换过程中的任何时间撤销文件，直至出版。要求保持文件在转换过程中不作任何改动也是认可的PAS 提交人的权利，这样的要求应当在说明性的报告中清楚地陈述出来。但是，在投票过程中改动规范是不允许的，因为这样容易造成混乱。”

5) NP 程序可以转为快速程序

JTC1 导则规定（JTC1 导则，第五版，第 56 页）：

“正如 12.1 中描述的，分委员会可以暂停正常程序，采用快速程序（由JTC1 P 成员或A 类联络组织启动），只要该分委员会一致认为拟定快速文件适用于满足现有项目要求；并且该分委员会一致同意使用快速程序并且将其通知JTC1。”

事实上， SC6、JTC1 以及 ISO/IEC 中央秘书处都已经同意将 WAPI 推进到快速程序。

6) 国家成员体可以在投票时建议改动

根据 JTC1 导则对快速流程投票的有关规定，国家成员体可以采取以下的投票方式（JTC1 导则，第五版，第 45 页）：

“不赞成 DIS（或 DAM），应说明技术理由，并附有使该文件可被接受的修改建议（这些建议的采纳意味相关国家成员体确认可将其投票改为赞成票）；”

既然投票可以建议修改，那么投票之前根据评论意见进行改动，也是合理的。

结论:

WAPI 是一种成熟的技术，WAPI 提案文本上的改动没有影响到它的技术结构和强度，这些改动是为了使它更适合成为国际标准以及在世界范围内的使用。所有改动都是根据评论期内的评论意见进行的，其目的是为了得到更多数人的赞同。除非有明显的证据可以证明 WAPI 有重大的安全漏洞，不能带来稳定可靠的安全解决方案，WAPI 为成为国际标准而进行的适应性的改动不应当受到质疑。

问题 #4: 定义了新的证书格式

某些评论说：*“JTC 1 N 7904 在条款 8.1.3 定义了一种新的数字证书格式。然而，是 ISO/IEC IS 9594 掌管着证书格式，这个主题不在 ISO/IEC IS 8802-11 修正案的范围内。JTC 1 N 7904 没有证明自己偏离*

了ISO/IEC IS 9594的内容是正当的。”

中方的回应：

事实上, 1N7904 (WAPI) 定义了两种证书格式。其中一种是X.509 v3证书格式（ISO标准）并且它是必备的。另一种是GBW证书格式，它是可选的。

因此，不存在WAPI证书格式与其它国际标准相冲突的问题。相反，WAPI 为WLAN证书格式提供了更多的选择。

问题 #5: WAI超范围

某些评论说: *“JTC 1 N 7904 在条款8.1.4.2 中定义了一种新的认证机制。然而，认证机制却不在ISO/IEC 8802-11 修正案的范围内。”*

中方的回应:

1) 同样，这不是一个新问题。在北京会议和法国会议上，IEEE提出了这一观点。中国国家成员体给出了合理的、有说服力的解释。（SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status）

2) WLAN安全需要WAI

WAPI 是一种新颖的、先进的安全机制，用以解决 WEP 的缺陷。WAPI 的创新技术观念在于对等端口控制和双向认证。

WAPI实现了MAC层的安全，WAPI中的证书机制仅是实现MAC层安全的手段。

此外，WAPI 的很多状态机是由 MAC 协议控制的，WAPI 和 MAC 协议已经形成密不可分的整体。

WAPI 解决了现有的 WEP 所带来的问题，是一套完整的机制。

3) 11i 中的 4 步握手协议与 802.1x 和 WAPI 有相似的情况

IEEE 802.11i 定义了 4 步握手协议，协议分组是封装在 MAC 层数据帧中的，根据同样的逻辑，4 步握手协议应不属于第一层和第二层的规范，也不应在 SC6 WG1 的范围之内。

此外，IEEE802.11i 采用 IEEE802.1x 作为认证协议，虽然 IEEE 802.1x 不在 IEEE 802.11i 的文本范围之内，它应被看作是 IEEE 802.11i 的必要组成部分。IEEE 802.1x 定义的分组同样封装在 MAC 层的数据帧中，根据同样的逻辑，IEEE 802.1x 应在 SC6/WG1 范围之外。而且，到目前为止，IEEE 802.1x 仅仅是 IEEE 的内部标准，而不是国际标准。

为什么没有人建议 IEEE 先提交 802.1x 到 ISO/IEC，在通过后再被 IEEE 802.11i 采用呢？这是不是双重标准？（中国国家成员体对 11i 的评论，参见 ISO_IEC_8802-11_2005_DAmd_6_Perceived Contradictions）

4) 我们相信物理的层次不应当被用来分解 WAPI

- 层次问题不应成为阻碍技术发展和妨碍急需的安全方案得到应用的障碍
- 对标准的评估应当基于技术需要和其带来的价值。
- 尤其是对于 WLAN, 提供一个安全的解决方案应当成为最首要的关注点和动机。
- 与其它国际标准相比，WAPI 并没有表现出任何难以解决的问

题。

结论:

因此，WAPI是专为解决无线局域网WEP的安全问题而设计的，它应在SC6 WG1的范围之内。并且，WAI是WAPI的主要组成部分，是解决WLAN系统问题的目前已知的优秀的技术。

国际社会需要一个及时的、值得信赖的安全解决方案。我们不能利用对程序问题吹毛求疵的解释，来阻止一个被迫切需要的技术进入国际社会。

问题 #6: 删除了 WEP

某些评论说: *“JTC 1 N 7904条款8删除WEP定义的做法与ISO/IEC 8802-11:2005的条款8.2冲突。采用JTC 1 N 7904会使得每个现存的仅使用WEP的设备不被兼容，这对国际标准来说是不期望看到的。这也意味着这些设备至少在某种权限上变得不合法，而不会对设备的拥有者做出任何补偿。”*

中方的回应:

1) 同样，这是一个老问题。中国国家成员体已经在北京会议和SC6 法国会议的有关文件中解释过了为什么没有在安全解决方案中保留 WEP。（参见 SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status）然而，为了使更多的人了解情况，我们将在本文档中再次作出解释。
2) WAPI 没有提供后向兼容性是基于安全方面的考虑，对安全性和安全强度的关注，是国际社会对没有被妥协的、可靠的安全

机制的一种需求。

3） 众所周知 WEP 存在严重的安全缺陷，被描述为“安全灾难”。它应该尽快被消灭。WAPI 是为提供更好的安全解决方案而替代 WEP 的。

4）中国专家指出任何向 WEP 提供后向兼容性的行为，是纯粹的向商业利益的妥协，减弱了安全保护的级别，使用户和网络容易受到各种攻击，从而导致对用户和市场的伤害。（详见 SC6WG1-SPV017-Item 8.5-SC6 WG1-CHN-004-Detailed Comments on IEEE 80211i）

5）为了保护过去的投资而保留 WEP，是一种在安全和商业投资之间做出权衡的做法，如果这种做法在 WLAN 国际标准安全机制中被接受，将是一种严重忽视消费者利益的行为。

6) 国际标准可以是国家的和地域性的标准，因此可以在重要的国家公共设施和基础建设中采用。标准可以在交通，金融，通讯，能源和其它国家网络中使用。折衷的安全解决方案可能使网络暴露在安全风险之中，使网络威胁国家安全。

7）在有可以保护消费者利益的新安全方案可用的时候，再进行这种折衷和妥协是不负责任的。未来的 WLAN 市场会是现在的成百上千倍，为了现在的市场利益而将未来更大的市场置于安全风险之中，是一种短视的行为。因此，提供一个不折衷的、可靠的、尽可能强度高的安全方案，将是最大的关注。

8）WAPI 就提供了这样一种解决方案。它可以同 11i 一起，作为一

个可选性解决方案，并且满足那些不想在 WLAN 系统中采用 WEP 的用户的需要。

9）对于“对这些设备拥有者的补偿”，这个话题不应该在此论坛内讨论。然而，这应该是那些制造、推进诸如 WEP 之类有缺陷的安全解决方案，并且使之市场化的人的责任。

结论：

WAPI 并没有提供与 WEP 的后向兼容性，因此保持了最高等级的安全，是那些愿意采用强健和可靠解决方案的用户的可选方案。国际社会应该看到这个战略性决策的好处，意识到仍然包含 WEP 问题的标准中存在的安全风险。

包含缺陷安全机制的国际标准不仅会伤害 ISO/IEC 的名声，还可能会削减它被国家和地区标准采用的机会。

<u>问题#7：WAPI 不符合 SC6-IEEE 合作过程</u>

评论说到：*ISO/IEC TR 8802-11:2001规定了JTC1/SC6/WG1和IEEE 802之间协作的方式，这是为了保证各成员“严格的技术评估”而制订的，包括ISO/IEC 国家成员体和IEEE 802。然而，JTC 1 N 7904是独自发展的，没有与社团共同发展的ISO/IEC IS 8802-11和修正案进行协调，因此不具有必要的“严格的技术评估”。*

中国的响应：

1） 这不是一个新的问题。这一直是 WAPI-11i 争论的焦点。在过

去几年内，这个争论已经由 **IEEE** 和一些国家成员体提出过很多次了。

2） 这个问题已经被解决了。**WAPI** 没有违反 **SC6-IEEE** 协作协议，**WAPI** 可以在 **ISO/IEC** 框架内继续发展，这已经在 **WAPI** 相关会议中多次做过决定了。

3） 在已经做出上述决定这么久之后，我们又看到这件事被重新提起。我们可以理解，一些没有参加过任何相关会议的国家成员体的确不了解情况。但是我们留意到美国国家成员体和英国国家成员体已经参加了有关会议（奥兰多会议、日内瓦会议和法国会议），并且同意了这些决定，竟然又重新提出这件事，这就非常令人愤慨了。

4） 中国国家成员体已经多次指出如下几点：

■我们尊重 IEEE，并且意识到它对 ISO/IEC 国际标准化所做的贡献。

■有很多中国专家参加 IEEE 活动。

■我们并不反对 SC6-IEEE 协议，但是我们反对对这个协议扩大化和错误地理解，以及人为地误导。

■我们已经邀请了 IEEE 来对 WAPI 评论。

■IEEE 已经提供了对 WAPI 提案的评论（奥兰多会议、法兰克福会议、日内瓦会议、北京会议、法国会议）。

■中国国家成员体（作为国家成员体）参加 IEEE 标准活动是不恰当，不切实际的。

■SC6-IEEE 协议并不适用于 WAPI 的具体情况。

■在 ISO/IEC 内，IEEE 并没有制定 WLAN 标准的专有权和垄断权。

■WAPI 必须在 ISO/IEC 内进行。

5） 在 2004 年，SC6 已经决定在 ISO/IEC 内发展 WAPI。

在中国国家成员体对于将 WAPI 提交给 IEEE 处理提出质疑后，这个决定已经在 2004 年 11 月奥兰多的 SC6 全会上做出了。SC6 文件提出（6N12765，SC6 2004 奥兰多全会，2004 年 11 月）：

“考虑到 ISO/IEC JTC1 SC6 和 IEEE 802 之间的协同工作，鼓励中国国家成员体将他们的特定提案提交给 JTC SC6 处理。这会保证提案会在适当的国际论坛内被评论，如果被采用，将作为 ISO/IEC 8802-11 工作而在国际团体内使用。”

这个文件在 SC6 奥兰多会议上一致通过了。

6） 日内瓦会议拒绝了 IEEE 的要求

5 月 17 日日内瓦会议的 IEEE 代表做出了另一个请求，希望把 WAPI 提交给 IEEE 处理。在中国代表团表达了关注和拒绝并经过多次讨论后，与会各方（中国国家成员体、IEEE 代表团、美国国家成员体、英国国家成员体、ISO/IEC 中央秘书处代表）一致同意在 ISO/IEC 框架内处理 WAPI。（详见日内瓦会议纪要）

7） 北京会议不允许 IEEE 做出类似的请求

尽管日内瓦会议已经形成了在 ISO/IEC 框架内处理 WAPI 的决议，但是此后，在北京会议之前，IEEE 再次作出了类似请求，希望在 IEEE 框架内处理 WAPI。然而，ISO/IEC 中央秘书处官员的观点

是既然此事已经决定了，就不允许对这个话题做出任何更多讨论了。

8） 法国会议决定在 ISO/IEC 内处理 WAPI

SC6 法国会议没有要求 WAPI 符合 SC6-IEEE 协议，而是将它的全部处理权限给了 ISO/IEC。

结论：

WAPI 并没有违反 SC6-IEEE 协议；协议并不适用于 WAPI；WAPI 确实收到了身为 C 级联络机构的 IEEE 的评论；WAPI 被 ISO/IEC 处理是合法的。

因此，SC6-IEEE 协议并不应该成为阻止 WAPI 在 ISO/IEC 内成为标准的基础。

中国国家成员体希望这是对此事的最终解释。如果有任何团体不接受这个解释，我们不排除要求 ISO/IEC TMB/SMB 做出最终规则来明确解决此事。

<u>问题 #8：WAPI 加密算法不公开</u>

评论说到：

“1 N 7904（WAPI）定义了一种新的加密算法，但却没有提供任何关于设计上或强健性的细节。这在 LAN（有线局域网）上已经被证明是很不好的方法，不能给人高可靠性的印象。”

中国的响应：

1） 这仍然是一个老问题。中国国家成员体在以前的会议上已经提供了对此问题的详细回应。在 2005 年 8 月 8-12 日的北京会议

上，中国国家体提供了一份文档，题目为“WAPI and Cipher Issue”（WAPI N33），它检查了关于标准加密算法的 ISO 有关政策。在 2005 年 8 月 31 到 9 月 2 日法国的 SC6 2005 全会上，中国 NB 进一步解释了文档中的问题，回顾了 WAPI 提案的状态。（SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status）

2） 在加密算法上没有国际标准。

3） ISO 委员会在 1985 年就认为加密算法太政治化了，并且决定不再继续进行加密算法的国际标准化。

4） 11i 将 AES 作为强制算法，因此使其成为事实上的国际标准，并且将其强加到国际社会内，这是令人质疑的。

5） 加密算法有敏感的政治色彩和安全限制。在很多国家都有法律和制度控制着加密算法。国际标准不应该取代这些法律和制度，而应该遵守它们。

6） WAPI 只定义了一种安全协议，没有定义任何密码算法，安全协议和密码算法之间的关系是相对独立的。1N7904 将 SMS4 作为可选的密码算法仅供参考，任何国家可根据当地的有关法律和规定采用不同的算法（例如 AES、TWOFISH、SEED 等），SMS4 算法属于北京数安科技公司 (BDST)，如果需要更多信息，请与北京数安科技公司联系(E-Mail: chinabdst@126.com)。因此，1N7904 没给对任何团体强加任何算法。

7） WAPI 已经提供了相关 ISO 标准规则（ISO9160）所需要的、关

于 SMS4 的必要信息。

8） WAPI 的加密算法协议并没有违反任何 ISO/IEC 标准规则。

9） 请求 SMS4 算法更加公开的请求不在 ISO/IEC 要求内，不能用于反对 WAPI 提案。

问题#9 ）中国将排除非 WAPI 兼容的产品

评论说到：*“如果 WAPI 成为 ISO 标准，中国将决定对非 WAPI 兼容的无线 LAN 产品关闭大门，而中国的制造厂商在从中国出口时将不会面临这种限制。”*

中国的响应：

1） 这不是一个新评论。在 8 月 8-12 日的北京会议中，有类似的争论。中国国家成员体做出了回应，问题也已经解决了。

2） 这是一个投机的假定，不是要讨论的合适的话题。

3） 有假定认为 WAPI 在中国发展是为了保护国内市场，这是不对的。WAPI 的目的是为无线通信系统提供增强的安全保护。ISO/IEC 8802-11 包含严重的安全缺陷，使得终端用户和重要的国家基础设置如通讯、交通、金融网络和一般公众暴露在各种安全风险之中。缺陷在公众和旨在保护国家安全的政府中引发了广泛的关注。为了消除 WLAN 标准中的安全漏洞，中国开始发展 WAPI 技术，在 2003 年 5 月将其作为强制标准引入。保护国家安全利益的这种措施并没有违反 WTO-TBT 协议。

4） 我们正在开发国际标准，而不是决定标准在国家和地区范围内

如何被采用和实施。

5） 国际标准是自愿性的标准。即使 WAPI 和任何其他提案成为了国际标准，它并不保证这些标准会在特定的国家和地区范围内被采用。有很多例如国家安全、性能、规则、规章、环境、以及反欺诈等诸多因素决定着这些标准如何实施及何时实施。

6） 在中国，WAPI 或其他标准是否被采用和实施，将决定于相关领域的国际规则，也决定于中国的需要和要求。

7） 中国国家成员体已经指出 WAPI 和 11i 并不互斥，他们都可以作为可选性解决方案而存在于 ISO/IEC 8802-11 内，在需要时被采用。本地需求和要求可能决定这些解决方案如何被实施。

8） 为了国际社会的安全和安宁，具有可靠安全性的，及时的安全解决方案将成为满足国际社会迫切需求的选择。

问题#10）WAPI 并没有得到中国领导层的全部支持

有评论指出：*“中国的 WAPI 支持者已经赢得了中国国家成员体的支持，但是有证据表明这个组织并没有获得中国部级领导层的支持。因此不支持 WAPI 标准不会必然地伤害与中国领导层的关系。”*

中国的响应：

中国国家成员体很震惊看到这个评论。我们对此信息的来源和真实性表示强烈怀疑和严重不满。中国国家成员体是中国在 ISO/IEC 的代表，下述所有立场和观点都由中国政府授权，我们在此声明：

1） 中国国家成员体要求看到所谓的“证据”。

2） 中国强烈不赞同此评论中表达的观点。

3） WAPI 是先进的、成熟的技术。它不仅仅有中国所有领导人的支持，也有 13 亿中国人民的支持。

4） 中国国家成员体已经在 SC6 法国会议中做出了声明（SC6WG1-SPV016-Item 8.3.2-SC6 WG1-CHN-003-WAPI Status）：*“WAPI 是先进的，成熟的技术。国际社会迫切需要这样的安全技术。中国政府和 13 亿中国人民强烈支持 WAPI。WAPI 是中国对国际社会的贡献。中国 NB 将 WAPI 作为可选性解决方案，它可以根据本地需要和要求而采用。WAPI 提案代表了广泛的观点，已经被修改以满足评论和建议。中国已经采用了数千个 ISO/IEC 标准。WAPI 应该从中国和 ISO/IEC 之间的互惠关系中获得。中国 NB 不觉得有任何理由阻止 WAPI 成为国际标准。出于所有考虑，WAPI 值得成为 ISO/IEC 标准。”*

结论：

中国对 WAPI 的完全支持是很清楚的，毫无疑问的。

6．结论

中国有良好的意愿和合理的原因来发展 WAPI 技术，将其作为国家标准，在任何合适的时间用其保护中国消费者和中国的安全利益，并且作为可选的安全解决方案将其提交为国际标准提案。中国已经对

包括WTO-TBT和ISO/IEC在内的相关国际规范和程序作了广泛而细致的研究，有自信认为这些考虑和活动都没有违反规则。中国提出WAPI不是为了制造贸易壁垒或保护国内市场，而是为了中国的信息安全，以及整个国际的信息安全。

中国政府有义务为我们的国家提供一个更安全的环境。中国不能让国家基础建设、公共设施和13亿中国人民受到恶意黑客和入侵者的攻击。

中国国家成员体相信本文档提供的以上的努力和信息已经完全解答了评论，解决了问题。

在目前阶段，中国国家成员体欢迎任何有疑问和顾虑的组织和团体能直接联系中国国家成员体，以建立有效的通话方式，从而达成完全的理解，达成令人满意的解决方案。

7．中国的其他观察

中国国家成员体也希望利用这个机会能表达最近与WAPI和11i相关事件的观察报告。

1） WAPI已经处于评论和持续的讨论中有1年多了，但是仍然有抱怨说国家成员体还是不能评论这个文档。

2） 我们理解有很多国家成员体没有兴趣和时间参加和 WAPI有关的国际会议，但有个很奇怪的现象，在过去的一年内，一直缺乏兴趣和参与；然而在9月7日到10月7日之间，突然就很热心提供评论。

3） 放弃参加 SC6 全会和 WG 会议，然后抱怨说他们的参与权被剥夺。

4） 即使在以前的文档和会议上已经做出了答案和解释，然而问题还是又一次被提出来了。

5） 以前会议的文档没有被阅读或仔细研究，在提供的文档中也没有考虑它们。

6） 即使在以前的正式决议中，类似的立场已经被拒绝，然而类似的立场又被提出。

7） 在不同场合下的立场转变。

8） 在这两个提案中，评论仅仅针对一个提案，而对另一个没有任何评价。

9） 在评论针对重大安全问题的提案中，对其中一个提案的非实质性的问题和传闻付出了极大的关注，同时却完全忽略了对另一个提案进行必要的分析，这显然是不公平、不公正的。

10） 对于评论一个提案使用了投机性假设。

11） 将传闻作为证据，影响了投票过程。

12） 根据应有的程序和一致通过的决议被推翻。

ISO/IEC 通过支持公平、公正、负责，和遵循既定过程的原则而建立了巨大的声誉和威望。中国国家成员体一直在努力维护这个传统。但是如上行动和行为违反了这个传统。中国将继续观察相关的发

展，在合适的时候采取必要的行动。

8．最后结论

在经过一年多认真审核，评论，讨论和陈述后，在考虑了部分评论意见，并对其余的问题和顾虑进行了有力的说服和详细的解释后，已经充分地证明，WAPI 是一个成熟、先进、可靠和合格的 ISO/IEC WLAN 标准的安全补篇。WAPI 满足了所有成为国际标准的要求，并且拥有中国政府和 13 亿人民的坚决支持。中国呼吁各国家成员体支持 WAPI 提案，使其成为一个安全可选方案，以帮助保护全球社会的信息安全。