中国国家成员体关于 IEEE 对 1N7904 评论意见的初步回复

美 IEEE 于 2005 年 11 月对投票期中的 ISO/IEC JTC 1N7904（中国 WAPI 安全提案）发表了评论意见。事实上 IEEE 提出的问题大部分是已在过去多次国际标准会议（SC6 奥兰多 2004 年会、SC6/WG1 法兰克福会议、ISO/IEC WAPI 北京特别会议、SC6 法国 2005 年会等）上讨论并澄清过，并已在 2005 年 12 月份中国国家成员体发给 ISO/IEC JTC1 各国家成员体的信件《China's Response to Contradiction Comments on 1N7904》中进行了再次充分解释的问题。

为进一步澄清相关问题，中国国家成员体将 IEEE 对 1N7904 的所有评论（共计 414 条）归纳为 9 个方面，下面是中国国家成员体对每一方面的初步分析和解释。

1、IEEE:"1N7904 技术上不完备，提案故意删除一些算法描述，包括分组加密算法的细节描述。"（10 条）

分析：

WAPI 安全协议的主体是唯一的，并充分考虑了密码学的知识，密码算法是可选的和可调用的项目。安全协议与密码算法是相对独立的，WAPI 安全协议可匹配多种可用的密码算法，密码算法只是一个被调用的模块，具体使用哪种密码算法应符合使用者的需要，并满足相应国家/地区的法律法规。

1N7904 中密码算法的处理方式与 1N7903（IEEE 802.11i）不同，1N7904 不要求使用者一定要使用包括中国算法在内的某个具体密码算法（包括对称加密算法和 ECC 算法的参数）。在 1N7904 中，使用何种密码算法是可选的，每个国家成员体可根据需要和各国不同的法律法规选择特定算法，以便使 ISO 的标准在最大程度上无障碍地得到应用。

当然，如果其他国家成员体愿意使用中国算法，也是可以的。在 1N7904 的附录 I（参考性附录）中列出了取得中国允许使用的密码算法的途径："详细信息可以与中国的数安科技公司(BDST)联系(E-Mail: chinabdst@126.com)。"

WAPI 提案允许不同的国家和地区根据自身的状况与需求选择合适的密码算法，为产品提供了更为灵活的适应性。况且 ISO 准则也没有要求提案必须对算法做出明确定义。IEEE 以此攻击 WAPI 提案技术不完备是不成立的。

需要指出的是，关于这一点，中国国家成员体在北京会议（N_33_WAPI_and_Cipher_issue_by_CNB_Beijing_Meeting_8-12_August_2005.pdf）和 SC6 法国 2005 年会（SC6 WG1-CHN-003-WAPI Status.doc）上均对此问题提供了详尽的书面答复。在这方面，WAPI 提案完全符合 ISO/IEC 规则和原则。我们认为这个问题已经获得恰当的解决。

2、IEEE: “1N7904 中定义的证书和协议分组超出 8802 标准系列的范围。” （11 条）

分析：

WAPI 是一种为 WLAN 设计的先进的、创新的安全机制，它的特点是对等接入控制和双向鉴别。WAPI 解决了 WEP 存在的严重安全问题，是一个完整的部分。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 实现了 MAC 层的安全，证书机制仅是实现 MAC 层安全接入的手段，应在 SC6 WG1 的 8802 范围之内。

另一方面，IEEE 802.11i 中定义了 4 步握手协议与 STAKey 握手协议，这些协议分组与 WAPI 协议分组同样均是封装在 MAC 层数据帧中的。根据 IEEE 的逻辑，假如 WAPI 不属于 8802 标准系列的范围，那 IEEE 802.11i 中的 4 步握手协议与 STAKey 握手协议也不应属于第一层和第二层的规范，即也不应在 SC6 WG1 的范围之内。

此外，IEEE 802.11i 采用 IEEE 802.1x 作为认证协议，虽然 IEEE 802.1x 没有直接编辑在 IEEE 802.11i 的文本中，但它应被看做是 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。并且，到目前为止，IEEE 802.1x 目前仅仅是 IEEE 的内部标准，而不是国际标准。那么，IEEE 802.1x 是否有必要先提交至 ISO/IEC，而在被批准后再被 IEEE 802.11i 采用呢？从这一点来讲，目前 IEEE 802.11i 是否根本就不具备 ISO/IEC 的提案要求呢？而如此具有行业较高水准、熟悉国际标准要求的 IEEE 为何做了这个提案，是否是一种故意行为呢？

IEEE 802.11i 既然没有包含超出 SC6 WG1 范围的技术内容，同样，专为解决无线局域网 WEP 的安全问题而设计的 WAPI 提案也应在 SC6 WG1 的范围之内。

需要指出的是，针对此问题，中国国家成员体已在北京会议和法国会议上分别提交文件予以说明。

3、IEEE: “1N7904 提案删除了 WEP 安全机制，无法保证后向兼容”。（14 条）

分析：

WEP有很多安全缺陷，并且很容易被攻击。在WLAN中允许使用这种技术，尽管不鼓励这种技术，但是仍然会将WLAN用户和网络置于安全风险之下。WEP的漏洞众所周知，从下述两个网页中可见一斑。http://www.winlab.rutgers.edu/pub/docs/JesseWalker.pdf与http://www.cs.umd.edu/~waa/wireless.pdf。

鉴于此，从信息安全和用户利益角度考虑，WAPI 没有提供与 WEP 的后向兼容性，以保障了其高安全性。WAPI 是那些愿意采用强健的、愿意为保障用户、产业和市场根本需要而努力，并认为为此应担负责任的厂商所选择的可靠安全解决方案。

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

针对此问题，中国国家成员体已经在北京会议和法国会议上分别提交文件予以说明。WAPI 并没有提供与旧的安全机制（如 WEP）的后向兼容性是基于认真考虑的，并且满足了不可妥协的、可靠的安全机制的需要。

4、IEEE: “1N7904 提案中存在编辑性错误、英文语法错误。” （223 条）

分析：

IEEE 认为，1N7904 存在英文描述和语法问题。

然而，我们想指出 IEEE 的态度和行为再一次破坏了 ISO/IEC 的规则和原则，根据这些规则和原则，这种编辑性事件应该在早期阶段提出，编辑性工作应该由工程编辑和编辑小组来完成。WAPI 已经在 18 个月前被阅读过，评论和修改过了。为什么 IEEE 一直等到投票开始才提出这些事情？为什么不组织编辑小组？谁在违反 ISO/IEC 相关政策？为什么？

答案是，IEEE 设置了语言陷阱，它一直等到投票开始才提出语言的问题，这样就可以使用语言作为武器来产生针对 WAPI 的反对投票了。这样在投票之后，WAPI 就会被延迟处理了。并且，出于这个原因，在 2005 年 SC6 法国年会上，IEEE 拒绝了中国希望形成编辑小组的提议。

5、IEEE: “1N7904 和 1N7903（IEEE 安全提案 11i）存在文本编辑性冲突，他们作为 ISO/IEC 8802-11 的补篇无法合并为一个文本。” （47 条）

分析：

针对此问题，曾经在 2005 年 8 月北京会议与 2005 年 9 月法国会议上进行了专题讨论，

中国国家成员体在北京会议上也给出了可行的文本合并方案（N_32_Introduction_of_the_CNB_Contributions__Beijing_Meeting_8-12_August_2005.pdf ），希望能够在三个月时间内通过双方的共同努力解决此问题。但 IEEE 坚持三个月时间内不可能完成，不同意和 WAPI 提案进行文本合并；IEEE 坚持 WAPI 提案中定义的协议分组超出了 8802 系列标准范围，不同意和 WAPI 提案进行文本合并；同时，IEEE 改变了在奥兰多会议上声明的“两个提案可并存”的说法，改口说两个提案是矛盾和冲突的，无法并存，不同意进行文本合并。甚至还提出，即使 IEEE 代表团同意文本合并，IEEE 的工程师也不会接受等荒谬观点。

按照 ISO/IEC 中央秘书处 9 月 6 日的决议，1N7904 和 1N7903 目前进入了独立并行投票阶段。中国国家成员体始终坚信这两个提案可以在国际标准中并存，并可以和 ISO/IEC 8802-11:2005 合并为一个文本。此问题可在投票分析阶段经过 IEEE 和中国成员体以及其他国家成员体一起共同讨论并开展文本工作解决。

6、IEEE: “1N7904 存在一些安全缺陷：BK 的导出方法和密钥协商过程使用的挑战。”（6 条）

分析：

（1） 关于 BK 和 BKID， BKID 可表示出当前使用 BK 是否变化，这不会带来安全威胁，因为安全协议分析已经假定攻击者具有该能力。

（2） 关于密钥协商挑战：攻击者必须截获 AE 的帧才能重放该帧，而如果 AE 发起协商而没有正确完成，AE 和 ASUE 的安全连接会被 AE 结束，AE 和 ASUE 都将删除 USKSA，该挑战将不再有效。

因此，说 1N7904 存在一些安全缺陷是不成立的。

7、IEEE“1N7904 不具有 ISO 标准快速流程资格”。（8 条）

分析：

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，并适应更多数的应用。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保障，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。同样的，为之进行的善意的努力不应被

夸大为不符合提案流程。

事实上，为此积极的改动也表明了中方在标准制定过程中，尊重并欢迎相关成员国提出意见和建议，同时也包括 IEEE。但这里需要申明的是，迄今为止包括 IEEE 在内没有国家成员体和标准组织提出对 WAPI 技术结构的置疑，而中方对 IEEE 的某些积极的但非 WAPI 技术结构的建议均给予了充分的考虑或采纳。

因此，认为 1N7904 不具有 ISO 标准快速流程资格是站不住脚的。

8、IEEE 对标准文本理解错误。（94 条）

分析：

IEEE 对 1N7904 文本理解上产生的错误多达 94 条。譬如 IEEE 提出，“The text states “there are two USKSAs at most…both may be active during rekeying process.” This description is incompatible with the USKSA data structure defined on page 28. In particular, the KeyIdx used by WPI to identify the USK is missing”事实上这个问题是由于 IEEE 对 1N7904 的理解肤浅的典型体现。在 1N7904 的第 28 页中定义了 USKSA 数据结构，其中包含用于标识 USK 的 USKID，同时，在第 66 页明确指出 WPI 的 KeyId 表示 USKID、MSKID 或者 STAKeyID，前后文的对应关系非常明确。因此，说“the KeyIdx used by WPI to identify the USK is missing” 是错误的。

这些问题表明，尽管 WAPI 被引入国际社会已经超过一年时间，但由于 IEEE 缺乏对 1N7904 的正确态度（使用各种手段将 WAPI 排除在国际社会之外），因此对 1N7904 技术和文本的理解上仍存在偏差。

9、IEEE 对专利问题提出的疑问。（1 条）

分析：

IEEE 提出“1N7904 在导言中进行了专利说明，但是由于导论不是 ISO/IEC 8802-11 修正案的一部分，因此需要提供一份完整的中国专利声明。…是否能以合理的非歧视性的条件而获得提出了疑问”。

而事实上，在 2005 年 8 月中国中国国家成员体在提交 1N7904 时，已经严格按照 ISO/IEC 以及 ITU 关于专利声明和许可的有关要求，向 ISO/IEC 提交了 1N7904 所涉专利的声明文件。文件中专利持有人明确表示“… …在全球范围的非歧视前提下，在合理的条件和条款下，向不限制数量的申请者提供许可”。

因此，这个问题早在 2005 年 8 月 1N7904 被提交时就已经解决了。

从以上的分析看出，IEEE 的评论意见绝大多数是在以前多次的相关会议中就已经被提出来的，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。以上针对 IEEE 评论意见，中国国家成员体提供了初步的总体答复，更详细的响应将在投票分析组会议上做出。

WAPI 提案提供了一个安全的、且能满足无线局域网安全需求的技术解决方案，该方案在无线局域网实际应用中更为灵活、更易管理和更为经济。国际社会迫切需要这样一种安全技术和任何为此所进行的努力，中国国家成员体始终欢迎任何对 WAPI 的评论。