For Immediate Release

Media contact:

Haiwei Bai

Marketing Director

atsec information security

haiwei@atsec.com

+86 01 84834011- 607

中国产品迎来 FIPS 140-2 合规认证丰收年

atsec，白海蔚

今年（2011 年）是中国厂商获得基于国际密码模块安全性相关的 FIPS 140-2 标准合规认证大获丰收的一年，atsec 先后与中兴通讯（ZTE）、皮尔森科技（Pierson）、握奇数据（Watchdata）等公司合作完成了 FIPS 140-2 的密码模块测试，并最终为这些公司的相关产品获得了由美国国家标准与技术委员会（NIST：National Institute of Standards and Technology）和加拿大通信安全局（CSEC：Communication Security Establishment of Canada）共同创建和维护的密码模块验证体系（CMVP：Cryptographic Module Validation Program）所颁发的合规证书。我们高度赞赏这些公司敢于尝试与开放严格的国际性标准的合规性检查，勇于接受第三方实验室基于标准的公正客观的测试和验证，研发团队勤于学习吸收标准精髓，善于改进产品安全性能，乐于做出不懈努力直至最终获得认证。通过认证的产品证书编号依次为#1586、#1589、#1634 和#1640，详细的验证结果可在如下链接查看：

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm

通过认证的四款产品既具有典型性又具有广泛性，产品形态涉及硬件和软件，产品类型包括用于网络设备以及管理软件中的提供密码支持的软件包、智能卡以及结合生物识别和令牌技术的硬件等，被认证的级别覆盖了 FIPS140-2 中规定的四个等级中的前三个。

在 FIPS 140-2 标准下获得密码模块的验证在许多行业和政府部门中越来越重要，目前世界上很多国家机构的采购和招标要求中也明确地提出具有密码模块的产品 FIPS 140-2 的合规要求。不仅仅是美国和加拿大，还包括全球很多国家。截至 2011 年 12 月 15 日，NIST 网站公布的已经获得 FIPS 140-2 认证证书的密码模块有 1655 个，而在 2011 年一年间 atsec 与中国厂商紧密合作使得在这些证书中包含了 4 个重要的来自中国大陆的产品。这对于我国国内的商业密码安全产品是一个里程碑似的跃进，特别是为其进一步打开国际市场提供了必要且重要的安全保障。

- 皮尔森的总经理 Frank Psaila 先生评论道：“该证书的获得对于皮尔森而言是一项巨大的成就，致力于该项目的工程师团队创造了前所未有的 FIPS 140-2 验证的记录，结合生物识别和令牌硬件，使其具有能力同时为 OTP 和 PKI 技术工作。对于在非常合理的项目周期内获得该项成功，在此对我们双方团

©2011 atsec information security

队的专家表示感谢。该成功将毫无疑问地为远程身份验证及其适用性设定新的标准，这也是该项目中我们的主要目标。”

- ZTE 美国首席执行官 CEO Lixin Cheng 在项目结束后这样说道：“ZTE 相信满足国际标准的要求是交付给来自客户要求的最为安全和可靠的解决方案的关键，获得 FIPS 140-2 标准的认证进一步展示了我们的工作，确保我们的研究和研发（R&D）战略映射了这些标准的重要性，使我们产品的质量和可靠性逐步赢得客户的信心。”

- 握奇数据副总裁高翔先生在项目结束后表示：“感谢 atsec 以及他们的辛苦工作，同时也感谢握奇数据的产品团队。该证书为握奇数据的 USB Token 迈向国际市场开辟了新的道路，但是这只是一个开始。未来将有更多的成功。”

正如来自厂商的声音，FIPS 140 认证的结果不但提升了客户对产品质量和可靠性的信心，而且为我国的产品走向国际市场开辟了新的道路。与此同时，atsec 密码和安全测试（CST：Cryptographic and Security Testing）实验室也因为成功完成这些首批来自中国大陆的产品的 FIPS 140-2 认证而骄傲。毫无疑问在整个测试和认证过程中，双方团队均面临着巨大的挑战，一方面这是国际上最为严格的、高质量的，且是广大中国的产品开发者所可能不是特别熟知的密码领域的信息安全标准，另一方面来自中国的前几个不同领域的产品认证申请得到了 NIST 较高级别的关注和非常高的审查要求。比如，在皮尔森 MIIKOO 设备评估过程中，因为产品采用的生物识别安全技术对于 NIST 认证是全新的，因而双方团队完成了独一无二的挑战，来证明其符合了 FIPS 140-2 安全级别为 3 级的标准要求。这些项目不仅要求广泛的技术知识和理解，atsec 测试人员必须全面探究 FIPS 140-2 标准的广度和深度，以展示其在这样高级别保障下的合规性。

经历了 FIPS 140 测评项目的洗礼，各个开发人员确实地体会到了该标准的实践为产品的信息安全和质量带来的提高，每一个合作的技术人员都深深地体会到了 atsec 对于致力于高质量和严格的信息安全保障要求的产品的专注和专业。针对此巨大成果以及与 atsec 的成功合作，我们也来听一下来自产品开发人员的声音：

- FIPS 140-2 认证终于取得了圆满的结果，这个和大家共同的努力是分不开的。在合作的过程中，atsec 实验室的贡献是有目共睹的，无论是熟练扎实的专业技能，严谨求实的工作态度，还是项目过程中对产品的每个细节不遗余力的反复推敲和确认，都体现出 atsec 作为一家业内领先的实验室在安全领域方面的的前瞻性和专业性。我们在认证过程中也都受益匪浅，对产品的安全性有了更进一层的认识。--握奇数据曹海涛

- 得到 Watchdata USB FIPS 140 认证通过的消息非常高兴！也非常感谢你们 atsec 团队在这一过程中的每一份帮助、支持与努力！虽然我是中途加入该项目组，但是已经能很好地体会到 atsec 在方案的分析评估、审查、修改建议等方面的高效与负责，争取到了很多时间以配合我们尽早完成测试与认证。在与 atsec 测试人员的配合中，我们也都深深感受到其认真、细致、高效、严谨，这也是我们在项目完成过程中提升 WatchSafe 产品的同时所学到的 atsec 令人佩服的工作态度，而且这个感受很深。这些因素都是帮助我们顺利获得认证的保证！我们也从中对产品的安全、文件结构的完善有了更多的改进和思考~谢谢！--握奇数据吕晓燕

- 回顾与我们与 atsec 共同完成的 FIPS 140-2 CAVP 与 CMVP 认证过程感触颇多，其中有几点仍记忆犹新。首先，站在产品设计的角度来说，使用 FIPS 140-2 认证标准来重新审视一款产品，这个体系标准从逻辑层到应用层，方方面面都有有法可循的具体要求，从而保障了产品的安全性能。其次，对于工程师来说，这套标准就是一套详细的设计大纲，从概要设计到详细模块设置，甚至到后期的功能，压力边缘测试都有具体的实施方案。所以个人感觉，工程师严格遵照认证标准实施下来，想设计出一个不安全的产品都很难。最后，真心的感谢 atsec 的同事们对我们项目的支持，没有你们的帮助，我们不能如此顺利的与远在地球另一边的美国实验室合作和沟通。--皮尔森李畅

©2011 atsec information security

- 感谢 Yi Mao 女士，在我印象中，她是一个非常忙碌的人，但纷繁复杂的事务并没有扰乱她的思维，在每周的例会中，她总是能做到思路清晰表达清楚，对 UEPCM FIPS 认证的进展和遇到的问题了如指掌，使我们能够非常清楚地知道当前要做的事情和下一步的工作计划。感谢 Trupti Shiralkar 女士，她主要负责 UEPCM FIPS 认证的相关文档审核以及测试的工作，她是一个非常专业而且严谨细心的人，对我们文档中不恰当的地方给出了详细的修改意见，减少了我们修改文档的次数，在进行 CMVP 远程测试的过程中，她经常工作到深夜，对不能满足要求的测试脚本进行修改，直到全部通过测试。感谢其他 atsec 的工作人员，虽然我们没有直接接触过，但你们科学的工作方法、严谨的工作作风以及坚持不懈的努力，为 UEPCM FIPS 认证成功做出了不可缺少的贡献，非常感谢！我期待与 atsec 的专家们再次合作！--中兴通讯胡江辉

早自 2007 年以来，atsec 已协助国民技术（原中兴集成电路）、杭州晟元芯片、时代今典、握奇数据、皮尔森等完成近 40 个算法的密码算法验证体系（CAVP ：Cryptographic Algorithm Validation Program）的测试和验证，详细证书信息请查看如下链接：http://csrc.nist.gov/groups/STM/cavp/validation.html

除此以外，atsec CST 实验室与全球诸多的大型厂商长期合作，开展基于 FIPS 140-2 标准的测试和认证，这些厂商包括但不限于三星、IBM、惠普、Red Hat、 Wind River 、Patrick Townsend Security Solutions、Quantum Corporation、Data Locker、Secuware 等。2011 年以来，在智能手机领域的密码算法和密码模块的测试得到全球诸多手机厂商的重视和投入，atsec 也期待着在这些新兴领域的更多的贡献。

atsec 作为全球化发展且专注在信息安全领域的独立评测和评估机构，在中国具有独立法人的实体和强大的本土专业团队，atsec 期待成为国内和国际的信息安全领域的桥梁，协助更多的中国客户获得国际信息安全领域的认证，提高产品质量和国际声誉！同时，atsec 也协助更多的全球的客户了解中国的信息安全标准要求。

关于 FIPS 140

FIPS 是美国联邦信息处理标准（Federal Information Processing Standard）的缩写。该标准描述了美国和加拿大联邦政府的敏感但非分类使用的信息技术产品应用的需求。FIPS 140-2 由美国标准与技术研究委员会（NIST：National Institute of Standards and Technology ）和加拿大通信安全局（CSEC：Communication Security Establishment of Canada）所维护的密码模块验证体系（CMVP：Cryptographic Module Validation Program）发布。这些标准和方针由 NIST 发布，并作为联邦信息处理标准（FIPS）在政府机构广泛采用，标准的合规针对美国和加拿大联邦政府采用的密码产品是强制的。NIST 针对强制性的联邦政府需求制定 FIPS 标准，比如安全和互操作性，同时针对那些尚未形成可接受的工业标准或解决方案的需求，制定 FIPS 标准。

如果机构指定信息或者数据受到密码保护，那么 FIPS 140-2 则被适用。FIPS 140-2 禁止在联邦系统中使用敏感或者重要数据的密码保护未经验证的密码系统。经过该标准符合性认证的产品模块将使其满足联邦政府以及相关机构的关于密码系统的技术要求。

关于 atsec 信息安全

艾特赛克信息安全（atsec information security）是一家独立且基于标准的信息技术（IT：Information Technology）安全服务公司（www.atsec.com），它很好地将商业导向的信息安全方法和深入的技术知识以及全球的经验相结合。atsec 在德国慕尼黑成立于 2000 年，并且通过美国、德国、瑞典和中国的办公室开展了广泛的国际业务。atsec 提供的服务包括正式的实验室测试和评估、独立的测试和评估以及信息安全咨询。

©2011 atsec information security

atsec 提供美国国家标准与技术研究委员会（NIST：National Institute of Standards and Technology）和加拿大通讯安全协会（CSEC：Communications Security Establishment Canada）制定的密码模块验证体系下的密码模块和算法测试服务。atsec 同时提供 NIST 个人身份验证体系（NPIVP）、密码算法测试（CAVP：Cryptographic Algorithm Validation Program）和安全内容自动化协议（SCAP：Security Content Automation Protocol Program）下的正式的测试，以及 GSA FIPS 201 EP 下的产品认可测试。

atsec 同时提供 PCI SSC 体系下的服务，并且是一家能够提供 PCI DSS 和 PA-DSS 标准的评估服务的 QSA 公司。atsec 的渗透测试、应用安全、ASV（Approved Scanning Vendor）服务和信息安全咨询服务，作为评估服务工作的有力支撑。atsec 是授权的 NASPO（North American Security Products Organization）第三方审计机构。

atsec 的客户包括全球首屈一指的公司如苹果、IBM、Hewlett and Packard、Samsung、Quantum Corporation、Red Hat、国民技术、握奇数据、华为和中兴通讯等，并一直维持密切合作关系。

©2011 atsec information security