atsec the information security provider
NEWS 05/2015

导读

最近新闻一览

更多的新闻，请参见我们的网站：
www.atsec.cn

您也可以关注atsec的官方微博
http://e.weibo.com/atsecchina

atsec 将分别出席 2015 VISA 安全峰会和 PCI 社区会议并设有展位

与往年一样，atsec将分别参加2015年度VISA安全峰会（VISA Security Summit）和PCI安全标准委员会社区会议（PCI SSC Community Meeting），并设有技术展位，呈现我们高质量的服务和技术储备。atsec专家将在PCI社区会议上发表题为“Improving Policy-Based Security Specification”的主题讲演。

2015年度会议信息：

- VISA亚太地区安全峰会将于2015年5月19日-21日在澳大利亚悉尼举办；
- PCI SSC亚太地区社区会议将于2015年10月14日-15日在日本东京举办。

atsec 出席第七届移动支付产业论坛并发表了 PCI 主题讲演

2015年4月22日，atsec受邀出席了在北京国宾酒店举办的2015年第七届中国移动支付产业论坛，并发表题为“PCI支付卡产业安全动态和最佳实践分享”的讲演。

详细内容参见：http://www.atsec.cn/cn/news--403.html

atsec 为中国信息安全测评领域同仁提供 CC 培训

2015年3月，atsec创始人、Common Criteria资深专家Staffan Persson受邀来到中国，为信息安全测评领域的产业同仁们提供了为期一周的Common Criteria（CC：通用评估准则）讲座。这位年近60岁的老人，饶有精神充满活力地分享了近30年来全球Common Criteria产品测评领域的变迁和发展，深入浅出的介绍了CC相关的政策、发展动态、以及技术要求。

atsec 圆满完成了支付卡产业数据安全标准 PCI 上海巡讲

2015 年 4 月底，atsec 成功举办支付卡产业 PCI 中国巡讲-上海站培训。atsec 与产业专家讲解了 PCI 的标准、技术要求和发展动态，并配合案例分析、实际研讨进行了深入的分享。来自支付行业的银行、支付机构、商户、以及专业技术机构等同仁积极参与，了解了最新且全面的 PCI 领域安全知识，且进行了较为深入的同行业技术交流。

请查询 atsec PCI SE 考核通过人员信息，并诚挚邀请继续关注 atsec 支付卡产业数据安全 PCI 标准巡讲-深圳站讯息。

atsec 中国完成华为云支付方案 CPS 的 PA DSS 合规评估

atsec中国很荣幸地宣布：2015年5月1日完成了华为技术有限公司（英文名称：Huawei Technologies Co.,Ltd.）（以下简称“华为”）支付应用系统云支付解决方案CPS（Cloud Payment Solution）基于支付卡行业（PCI：Payment Card Industry）的支付应用数据安全标准（PA DSS：Payment Application Data Security Standard）v3.0版本的合规评估，并且通过了支付卡产业安全标准委员会（PCI SSC：Payment Card Industry Security Standards Council）的验证。

成功的评估验证结果发布在PCI 安全标准委员会（SSC：Security Standard Council）官方网站上，链接如下：https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php?agree=true。参见下图显示了PCI SSC官方合规列表：

Huawei Technologies Co., Ltd.

CPS (Cloud Payment Solution)

Version #: CPS V100R001C30M0101 **App Type:** Card-Not-Present **Target Market:** mobile payment, e-commerce **Reference #:** 15-10.00989.001 **Tested Platforms/Operating Systems:** SUSE Enterprise **Service Pack/Build/Version:** V11.0	Validated According to PA-DSS *(PA-DSS v3.0)*	Acceptable for New Deployments	1 May 2016	28 Oct 2019	atsec (Beijing) Information Technology Co., Ltd

atsec 中国成功完成航空结算 PCI DSS 年度合规评估

中国航空结算有限责任公司（以下简称“航空结算”）于2015年3月30日通过了atsec基于支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standards）v 3.0版本的符合性评估，这也是航空结算首次通过PCI DSS数据安全标准符合性评估。

对于本次PCI合规的成功合作，航空结算总经理郭天表示：“为提升新航国际客运、BSP、第三方支付等信用卡交易数据安全性，提高其信息网络系统高稳定性，结算公司以PCI DSS合规性建设为契机，组建了包括研发、运维、支持在内的28人专门项目团队，投入了约480人月，针对数据输入、处理、传输、存储、备份、恢复、演练等各个环节，覆盖系统设计、研发、运行和审计等四维空间，开展了整套的数据安全性建设。我们通过实施三大业务信息网络系统的合规性建设，全面夯实了信息安全建设基础，全面提升了数据安全保障水平，属交通运输业内首次大规模、整业务、成系统实施，获得新加坡航空公司、国际航协、中国人民银行的高度认可，并取得了重大的经济效益”。

atsec中国PCI实验室副主任和资深顾问高向东评论到：“PCI DSS作为业界公认的数据安全标准，其对于持卡人数据的保护能力和可信度正被全球范围内越来越多的机构所认可。涉及处理支付数据的机构，尤其是涉及持卡人数据处理的机构，符合PCI DSS标准将是一个向其合作伙伴和监管机构进行安全技术和安全管理保护能力的一个有效方式。我们在此向航空结算表示祝贺，也希望通过PCI合规促进越来越多的合规机构能更多地参与到国际性的业务合作，并且提高自身的信息安全管理和技术水平。在此过程中，atsec也将持续地尽最大努力提供服务，以帮助合规机构不断提升安全技术与管理方面的能力。

唯品会支付系统成功通过 atsec 基于 PCI DSS 安全评估

广州唯品会网络科技有限公司（以下简称“唯品会”）于2015年4月16日通过了atsec基于支付卡产业数据安全标准（PCI DSS）v 3.0版本的符合性评估，这也标志着唯品会的支付系统成功通过PCI DSS数据安全标准符合性评估。

对于本次PCI合规性评估的成功，唯品会相关负责人表示：“唯品会顺利的通过PCI的合规评估，标志着唯品会支付系统的建设达到了新的高度。在这次评测中，atsec方面的专业团队带来丰富的支付系统合规建设意见，有利于唯品会进一步快速提升支付系统的安全保障能力。希望双方未来继续加强合作，共同维护唯品会支付系统的合规建设。”

atsec中国总经理及PCI实验室主任刘岩表示：“我们赞许唯品会在从事支付业务对于数据安全保护的重视，并积极主动地致力于PCI的合规性建设和第三方安全评估，也非常感谢技术团队和管理层在整个合规评估过程中的大力配合。越来越多的电子商务和新兴的业务领域涉及到电子支付，同时支付的方式和技术也在飞速的发展，而对于数据安全保护，特别是涉及金融资金交易的安全性是任何机构和业务得以长期且稳定发展的根基。我们也鼓励更多的电子商务机构投入到PCI安全建设中，打造更加健康可靠的支付生态环境。”

国际 CC 认证体系和 CCRA 简介

刘岩，atsec 中国，2015 年 4 月

关键词：产品安全评估、通用评估准则、Common Criteria

标准历史和发展

通用评估准则（Common Criteria，以下简称CC）标准源于世界多个国家的信息安全的准则规范，包括欧洲ITSEC、美国TCSEC（桔皮书）、加拿大CTCPEC以及美国的联邦准则（Federal Criteria）等。这些准则规范在CC发展历程上均得到了各国大力支持，因为早在CC制定之初便达成了共识：采用一套公共的准则规范为IT保障类产品的广泛用户群体提供最大的便利。CC标准很有意义的贡献之一便是将安全功能需求（Security functional requirements）和安全保障需求（Security assurance requirements）通过标准独立的两个部分分开（Part2和Part3）。评估将在特定的安全功能要求上选择适合产品自身条件和产品用户要求的安全保障需求，或者选择预定义的安全保障级别（EAL）。

国际CC标准由专门的CC开发组（CCDB）负责开发和维护。1998年，标准开发组的参与国联合了其他国家共同签署了CC互认协定（CCRA）[1]，其中协定很重要的部分是明确了该体系下认证产品可以得到广泛的认可，目前互认的安全保障级别（EAL）最高为4级。该协定组织明确规定了CC和CC评估方法论（CEM：Common Evaluation Methodology）作为互认协定所使用的标准基础。

除此之外，许多尚未加入到互认协定的国家和机构，也将CC作为关键的标准进行使用，并对CC的发展起到了重要的作用。经过国际范围的不断审核，国际标准组织（ISO）正式采纳CC标准为ISO/IEC 15408（Parts 1-3），CEM为ISO/IEC 18045。CC标准不仅仅用于CCRA成员国家 [1]，还广泛应用于其它国家和地区，例如欧盟范围所采用的另一个认可体系SOGIS。中国引入了ISO/IEC 15408标准作为GB/T 18336国家标准，但中国目前并没有加入到CCRA。

目前CC标准已经发展到第三版本，最新版本为CC v3.1，并于2006年年底正式被国际体系所采用。2008年所发布的中国国家标准GB/T 18336等同采用CC 2.3版本（也即ISO/IEC 15408：2005），目前国际CC产业已经停止了CC 2.3版本的使用，完全采用最新版本的3.1版本。

标准概述

CC是专注于信息安全领域且具有奠基意义的一部标准。在标准所定义的同一个框架内，使用的是同一种专业语言，使得计算机信息产品的使用者能够用严格规范的方式来明确提出产品的安全功能的要求。同时，产品的研发商能进而实现这些所要求的安全功能或是声明他们的产品具有怎样的安全特性，实验室的测试评估人员也能评测产品是否真正地达到了研发商所宣称的安全功能。由此可以看出，CC是为计算机信息产品的安全功能说明、实现以及评估提供安全保证的一部通用标准。

CC在标准结构和撰写形式上一共包含三个部分，就像是一本书的三个大章。这三个部分在内容上可以说是唇齿相依、融会贯通、缺一不可的，如果其中任何一个部分被孤立起来，则不能独立地构成一个有任何应用价值的标准，孤立的部分也无法确保产品的安全性能有效地被评估出来。为了更清晰地说明三部分间的关系，每一部分说明如下：

CC第一部分介绍了CC的基本思路和一般模型，定义了评估目标（Target of Evaluation，简称TOE）、安全目标（Security Target，简称ST）和保护轮廓（Protection Profile，简称PP）这些重要的基本概念，并且规定了撰写ST和PP这类文档的格式及要点。评估目标简单说来就是要对此进行评估的对象产品。安全目标是对某个特定的评估目标提出的要其满足的安全功能要求（Security Functional Requirements，简称SFR）和安全保障要求（Security Assurance Requirements，简称SAR）。保护轮廓是对某一类产品提出的安全功能和安全保障要求。

CC第二部分详细描述了可供ST或PP选用的安全功能组件，共分十一个大类，其中有安全审计、通信、密码支持、用户数据保护、标识和鉴别、安全管理、隐秘、TSF保护、资源利用、TOE访问和可信路径/信道。每一大类内，又逐步细分到不同的族、组件及组成要素。CC第二部分提供的安全功能组件集合了当前信息安全产业界最普遍使用的技术方法，是非常有价值的可供参考的安全功能描述。然而，CC第二部分既不强迫任何产品必须选用一些特定的安全功能组件，也不能保

证所有信息安全产品所需的安全功能都已存在相应描述。CC是有弹性可扩展的框架性体系，它允许ST或PP的作者按照CC第二部分提供的对已定义的安全功能组件的格式来定义描述新的安全功能组件。

CC第三部分详细描述了可供ST或PP选用的安全保障要求。安全保障要求覆盖到对ST的评估准则、TOE的开发、生命周期支持、指导性文件、测试、脆弱性评定在内的六个方面。根据在每个方面安全保障要求的数量多少和松紧程度，CC第三部分中又定义了七个评估保障级（Evaluation Assurance Level，简称EAL），每个评估保障级都是将六个方面的安全保障要求的细节按一定方式搭配并固定下来。从EAL1到EAL7，在六个方面的安全保障要求由少到多、由松到紧逐渐递增。

CC评估具有两个重要环节。第一步是对确定的安全目标的评估。安全目标可以遵从于某个保护轮廓（Protection Profile，简称PP），也可以没有遵从的保护轮廓而是针对某个特定产品撰写的。提出安全目标和保护轮廓的基本准则是根据某个或某类产品需要保护的信息资源的价值，以及此（类）产品使用环境受到敌意攻击的威胁程度，来选取合适的安全功能组件和安全保障级别。如果此（类）产品实现了所要求的安全功能组件，并且这些功能的设计和实现是达到了所要求的安全保障级别的，那么从理论（即CC的理想）上讲此（类）产品有能力抵御来自所处的使用环境的威胁，因而能够有效保护所拥有的信息资产。安全目标的制定应符合CC标准的第一部分一般威胁模型的方法。

CC评估的第二步是对安全目标中所定义的TOE的评估。这一步的评估要点在于通过对产品的设计文档、代码实现、生产流程、使用安装、功能测试、脆弱性分析等等多个角度和方面来衡量判定此产品是否真正地实现了在其ST中所宣称的安全功能，是否真正地达到了所宣称的安全保障级。这里要强调指出的是，ST中指定的安全保障级中包含的安全保障要求将贯彻覆盖到所选用的全部的安全功能组件。

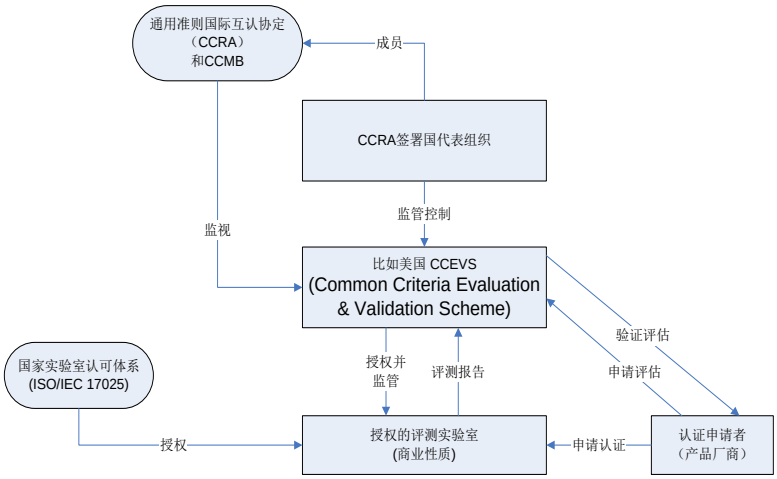
对于EAL1到EAL4的CC评估，CCRA还发布了通用标准评估方法论（Common Criteria Evaluation Methodology，简称CEM），并被接纳为国际标准ISO/IEC 18405。据作者所知，中国信息安全领域的专家们对CEM已作了中文翻译，目前尚未看到该部分发布为一个国家标准。

概括来讲，CC评估是基于CC第一部分提出安全威胁模型，该模型根据产品面临的安全问题（假定、威胁和组织安全策略），确定安全目标，并根据CC第二部分的安全功能要求选择产品的安全功能，基于CC第三部分的安全保障要求开展CC评估。

认证体系

截至2015年4月份，CCRA成员国总计26个国家，其中已有17个国家的相关政府机构拥有自己的评估认证体系可进行认证证书的颁发并接受互认（Certificate authorizing），它们是澳大利亚、加拿大、法国、德国、印度、意大利、日本、马来西亚、荷兰、新西兰、挪威、韩国、西班牙、瑞典、土耳其、英国和美国；而另外的9个国家可以接受和认可来自上述国家颁发的认证结果（Certificate consuming），它们是奥地利、捷克、丹麦、芬兰、希腊、匈牙利、以色列、巴基斯坦、新加坡。

如下图所示，CCRA各个成员国家所采用CC评估和认证体系均设有认证机构和授权的评估实验室，他们与评估发起者（申请者）合作完成产品的评估和认证。



图：国际CCRA评估和认证体系

在 CCRA 体系中，成员国家的相关政府职能机构负责签署互认协定并最终成为成员国家，同时其认证机构需要在 CCRA 监管之下开展工作。

而CCRA体系，管理职责一方面由CCRA承担，通过周期性审核评定确保各个国家测评认证体系的质量，该任务基于CCRA附录D、附录G.3、以及附录H的要求说明开展工作。另一方面由国家层面的管理职能机构负责，比如美国体系下，其CC评估与认证体系（CCEVS）是美国国家信息安全保障合作组织（NIAP）的一部分，而NIAP则隶属于美国国防部（DoD）下属的国家安全部（NSA）的信息保障部门。在德国，CC评测认证体系由德国BSI（The Bundesamt fur Sicherheit in der Informationstechnik）负责开展，总部位于波恩（Bonn）的德国BSI机构成立于1991年，该机构作为德国联邦政府的IT安全权威部门，协同德国内部和国际合作伙伴负责全面的信息安全工作，如密码、网络安全以及各类相关认证。

各个国家评测实验室的授权和认可工作都十分的谨慎和严格，如CCRA等相关文件规定，需要遵从一系列的审核以及符合性要求，例如ISO/IEC 17025针对测评实验室的授权要求。CCRA体系之下，美国的CC评测实验室授权工作是由美国国家标准和技术学会（NIST）下属的国家实验室自愿认可组织（NVLAP）联合NIAP共同展开的。截至2015年4月，美国体系下授权评测实验室共计9家，包括atsec information security corporation等。德国BSI体系下的评测实验室共有9家，包括atsec information security GmbH等。下图展示了CCRA文件中提及的实验室需要符合ISO/IEC 17025实验室的管理和技术要求：

a) the *Evaluation Facility*

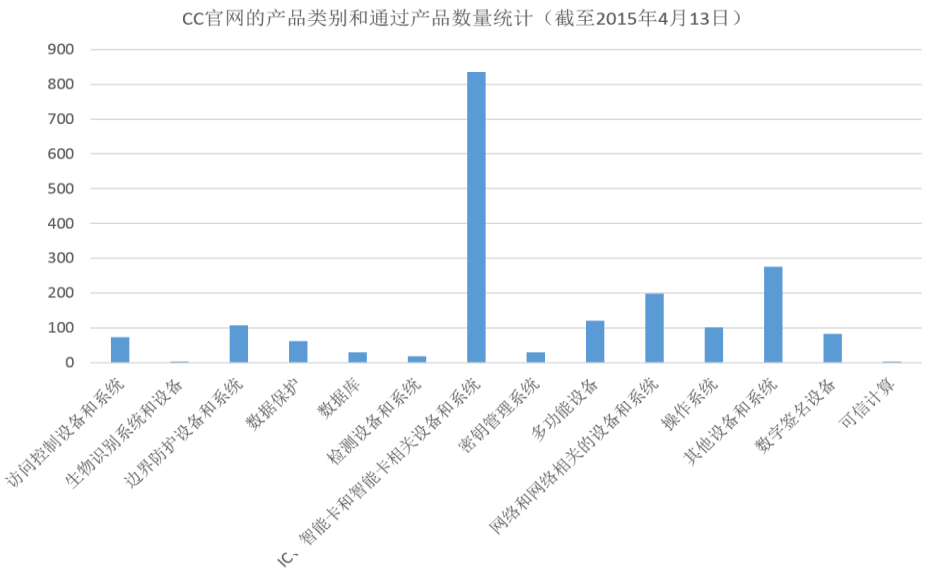
- either has been *Accredited* in its respective country by a Recognised *Accreditation Body* in accordance with ISO/IEC 17025, its successors, or in accordance with an interpretation thereof approved by all Participants, and has been *Licensed* or *Approved* in accordance with Annex B.3,

在美国和德国等国际CC评估体系下，认证机构（CB）并不直接为评估申请者进行产品评测，而评测工作由上述授权的商业评测机构来完成，例如美国CCEVS和德国BSI，作为CB只负责产品的认证，对评估机构提供结果的审核，以及对评估机构的定期监督审计和监管。而对于评估申请者（一般是产品厂商），需要与评测实验室直接联络来完成评测认证工作。

认证活动

CC标准的面向对象是信息技术产品的安全性。面对各个类型的产品。只要该产品具有安全功能，则可以采用这个标准致力于安全测评和评估工作。

基于CCRA体系由CCRA官方网站数据显示的产品认证情况如下图所示[2]。



图：国际CCRA体系产品认证分类图

下表显示了国际体系的一些认证结果数据。CCRA的数据来源于CC官方网站所显示的列表，其中显示仅限截至2015年4月13日官方所公布的产品信息，也不包括EAL5或者更高级别的产品；另外有些认证申请者由于机密性考虑，要求不公开其证书和产品信息，故而此统计数据也不包括这些产品。

	评测实验室个数	完成认证产品总数
澳大利亚	2	60
加拿大	4	233
法国	5	490
德国	9	565
意大利	4	12
日本	5	169
马来西亚	2	19
荷兰	1	34
挪威	4	44
韩国	7	76
西班牙	3	61
瑞典	2	12
土耳其	3	19
英国	3	29
美国	9	113
CCRA 合计	63	1939

国际CC会议和CCUF

每年度的国际CC会议（ICCC：International Common Criteria Conference）吸引了来自认证机构、评估实验室、厂商、最终用户、以及研究机构的诸多专家前来参加。自2000年第一届CC会议在美国召开的15年来，CC会议分别在英国、加拿大、瑞典、德国、日本、西班牙、意大利、韩国、挪威、土耳其、马来西亚、法国、美国、印度，2015年的ICCC将在英国举办。

此外，atsec和产业长期以来一直在呼吁CC标准的发展应该吸取更多来自最终客户的声音，故而2012年CC用户论坛（CCUF：Common Criteria User Forum）正式启用，并定期召集产业展开技术研讨，旨在提供产业各方更好的交流平台。参见：http://www.ccusersforum.org/。

结束语

本文简要地描述了CC标准的国际使用情况和现状。无论是CC认证机构、评估机构，还是产品开发者、产品最终用户，整个产业均理解和认可高质量的CC评估的真正价值和意义，他们对于标准的发展也起到了至关重要的作用，比如目前国内外很多切实从产品用户需求角度提出的经典的保护轮廓（PP）被广为采纳和使用。

来自中国的CC领域专家已经和国际CC组织开展了很多技术层面的交流，相信通过各国的共同努力，产品认证体系和测评标准会进一步的完善和提高。atsec作为专注在信息安全领域中立的测评机构，也很高兴能够成为世界和中国信息安全产业的桥梁，为信息安全保障做出我们的贡献。

更多的相关CC的资源和信息，可以参见atsec官方网站：

http://www.atsec.cn/cn/common-criteria-laboratory.html

参考文献：

[1] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014

[2] CC 官方网站 http://www.commoncriteriaportal.org

[3] atsec CC 官方网站 http://www.atsec.cn/cn/common-criteria-laboratory.html

采用 OTTPS 保护供应链安全

谢继来、刘岩，atsec 中国，2015 年 3 月

关键词：供应链安全、安全评估、OTTPS

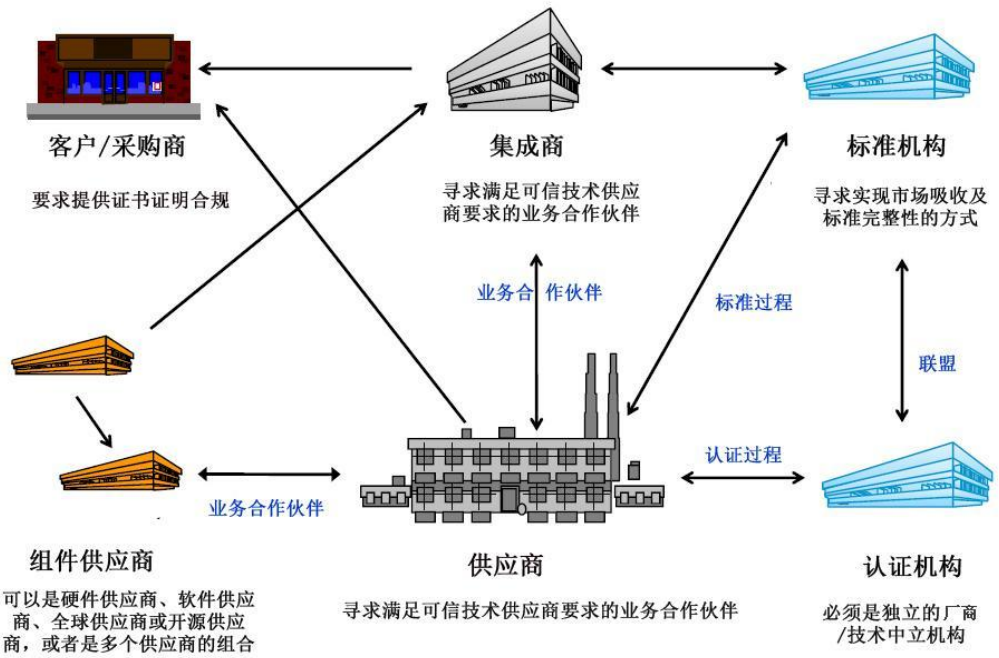
开放可信技术供应商标准（O-TTPS）是一套用来解决商用现货（COTS）与信息通信技术（ICT）产品整个生命周期内软硬件完整性威胁的指南、要求以及建议。

当今采购商在其 COTS ICT 采购中面临如下的两大威胁：

1. 受恶意污染的产品，即产品由供应商生产且经供应商授权的渠道购得，但产品已被恶意篡改。
2. 伪冒产品，即产品并非由供应商生产，或并非为供应商生产，或由未经供应商授权的渠道提供给供应商并被包装为合法正规产品（尽管其并不是合法正规产品）。

本标准的该初始版本用于解决与被恶意污染的产品及伪冒产品相关的威胁。

经营场景示意图:



经营场景相关方解释：

标准机构：开发某些认证标准及技术规范的组织。 本标准(OTTPS) 由国际开放标准组织可信技术论坛（The Open Group[1] Trusted Technology Forum）简称“OTTF[2]” 制定。

认证机构：提供认证与/或测试服务，尤其是参与合规性认证与/或测试的机构。 atsec[3]是全球首批 OTTPS 认证体系的认可评估机构。atsec 从标准制定之初便积极参与了该标准的编写工作，且由 atsec 中国主导完成了该标准的中文版本的翻译和完善工作。

客户/采购商：从组件供应商、产品供应商或集成商处采购产品或服务。

集成商：为客户提供服务及解决方案。 这些服务及解决方案一般用于涉及多个供应商的大型项目。

供应商：构造产品，包括公司内部的产品或供应商提供的软件与/硬件组件。

组件供应商：组件供应商一般作为供应商的业务合作伙伴。

本标准要求供应商，组件供应商遵守 O-TTPS 标准要求及被认证为可信技术供应商，而客户/采购商及集成商则可以寻求可信技术供应商提供的产品或业务合作伙伴。

OTTPS 合规的目标及效益

技术供应链日益向全球化、分割化及专业化方向发展。 所有商业及政府采购商、集成商、软件开发商、硬件供应商及生产商都是全球技术供应链的成员。 因此，全球社区的各个成员有责任确保端到端技术供应链的安全性。

OTTPS 合规可以使下列各方受益：

- **供应商：**采用这些实践的供应商能够在 COTS ICT 产品的开发、采购及维护流程中更好地识别及消减安全风险。 这些供应商能够利用与可信技术供应商身份相关的市场区分点，更轻易地从自己的供应商及商业合作关系中识别可信技术供应商。
- **组件供应商：**遵循最佳实践要求及建议的供应商还可获得可信技术供应商身份，能够充分利用与该身份相关的市场区分点，便于可信技术供应商及集成商之间结成更加密切、更加频繁的商业合作关系。
- **集成商：**集成商可从可信技术供应商及组件供应商处购买产品及组件（包括软件及硬件），促使基于外包及合作伙伴关系的集成工作变得更加安全、可信。 除此之外，遵守 O-TTPS 及作为可信技术供应商的集成商可以获得与上述供应商相同的利益。
- **采购商：**采购商可将供应商遵守 O-TTPS 作为其综合商业技术采购及风险管理策略的组成相关方之一。
- **整体市场：**随着时间的推移，OTTF 工作产品的广泛应用与/或参考可按照促进信赖、责任感及全球创新的方式，帮助巩固全球信息技术设施的安全性。

总体实施方法

1、准备阶段：

准备分析：atsec 顾问将与机构协同工作，提供 O-TTPS 标准和认证体系的介绍。通过与机构关键岗位进行会谈，我们将帮助识别不符合该标准的主要差距，并帮助制定成功完成该认证的合理战略。

实施选择准则申请（ISCA：Implementation Selection Criteria Application）:确定认证范围，完成 ISCA 模板。

证据整理和完善：收集整理认证所需的证据，该证据将用于提供给 O-TTPS 认可评估机构。

O-TTPS 培训：atsec 可以为机构提供相关的技术培训。

2、认证阶段：

atsec 作为国际开放标准组织 O-TTPS 认证体系的授权认可的评估机构，将执行认证体系所规定的如下评估活动：

- 审核所提交的认证包是否符合 O-TTPS 要求
- 基于机构提供的证据执行评估
- 基于成功评估结果向认证授权（Accreditation Authority）机构提出通过认证的建议

正确的实现合规，该标准能够减少整个 COTS ICT 产品生命周期中获取恶意污染或假冒伪劣产品的风险，产品生命周期包括如下阶段：设计（design）、采购（sourcing）、构造（build）、实施（fulfillment）、分发（distribution）、维护（sustainment）和处置（disposal）。自愿性 O-TTPS 认证体系的符合性的展示提供了机构符合该业界标准的正式的认可，并且允许机构声明其为可信技术提供商 Open Trusted Technology Provider TM。

更多信息可以参见 atsec 网站信息：http://www.atsec.cn/cn/o-ttps.html

[1] Open Group 的认证图标是商标，且 The Open Group 是国际开放标准组织（The Open Group）的注册商标

[2] 国际开放标准组织可信技术论坛（The Open Group Trusted Technology Forum，简称“OTTF”或“论坛”）是一项旨在邀请行业、政府及其他感兴趣的参与者共同推进本标准及其他 OTTF 可交付成果的全球行动。

[3] atsec 信息安全是开放标准组织 O-TTPS 认证体系注册认可评估机构

PA DSS 3.0 标准更新解读

作者：张力（atsec 中国）

关键词：PCI -DSS、PA-DSS、安全评估

1. PCI-DSS标准家族介绍

如我们所知，PCI-DSS标准家族主要由三部分组成，分别是PCI-DSS（Payment Card Industry Data Security Standard）、PA-DSS（Payment Application DataSecurity Standard）与PTS（PIN Transaction Security），PCI-DSS标准主要关注于持卡人数据环境的安全，PTS关注于ATM或POS机进行支付交易处理时PIN码及其相关密钥的保护，而PA-DSS则关注于整个支付应用软件的安全，使其更容易地部署在持卡人数据环境中，以支持持卡人数据环境合规于PCI-DSS的安全要求。

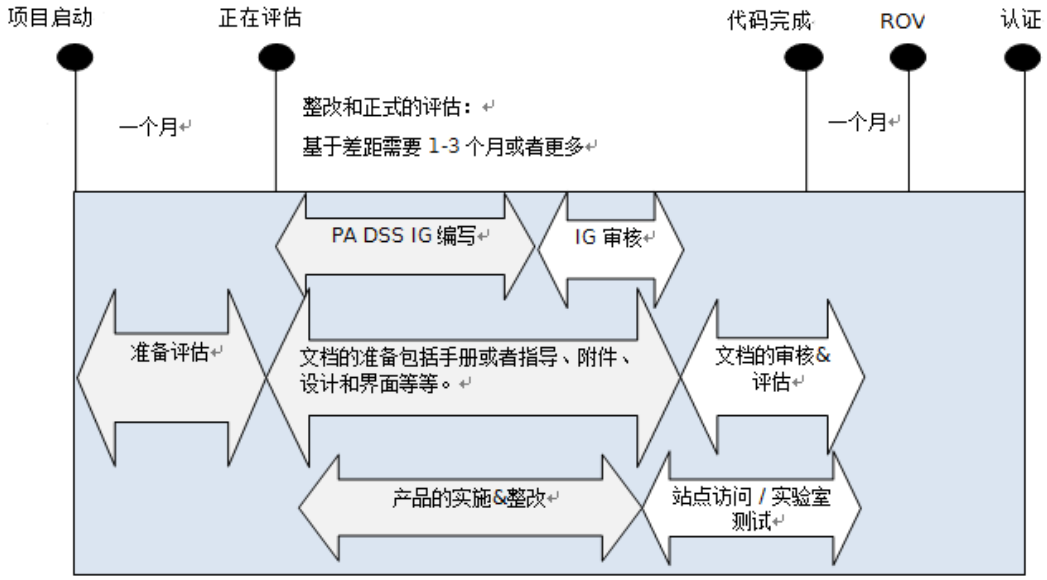
2. PA-DSS 3.0 适用场景

如果商用的支付应用软件存储、处理或传输持卡人数据，并且将其作为授权或结算操作的部分，则适用于PA-DSS标准。

支付应用类型	PA-DSS 适用吗?
非定制的商用支付应用软件	适用
支付应用模块	适用 注：通常是基于最佳实践的考虑，将支付功能集中到一个或少量的基本模块，而其他模块执行非支付功能。
支付应用是提供给客户的一种服务，为服务提供商所拥有。客户没有能力管理、安装或控制这种支付应用或它的环境。这种支付应用不被销售或授权给第三方。	不适用 注：此种支付应用应由服务提供商自己的PCI-DSS审核所覆盖。
为某一客户定制开发的支付应用	不适用
由商户或服务提供商开发内部使用、不销售给第三方的支付应用	不适用 注：此种支付应用应由商户或服务提供商自己的PCI-DSS审核所覆盖。
安装支付应用的支持系统，比如数据库、操作系统、平台系统等。	不适用

3. PA-DSS评估简介

如下图所示，PA-DSS评估大体可以分为四个阶段。第一个阶段是准备评估阶段，atsec开发了完整先进的准备评估的方法论，可以协助客户明确支付应用的审核边界，并共同识别差距，提出详细的整改建议。第二个阶段是基于差距的整改以及实施指南IG（Implementation Guide）的编写，这个阶段的周期通常根据支付应用的现状差距和整改的工作量等因素有所不同。第三个阶段是正式评估阶段，具有资质的评估人员QSA将开展全面的合规评估，之后出具ROV（Report On Validation）报告和AOC (Attestation Of Validation)证明。第四阶段是提交IG、ROV与AOC给PCI标委会审核，审核通过后PCI标委会将通过PCI官网发布认证结果。



图：PA-DSS 评估参考示意

4. PA-DSS 3.0 相对2.0的更新

PCI安全标准委员会于2014年初发布了PA-DSS 2.0的更新版本PA-DSS 3.0，相比PA-DSS 2.0，PA-DSS 3.0做了一些重要的变化与补充以适应不断发展的风险管理，融入了安全的最佳实践。在PCI 安全标准委员会的官方网站上，有一个标题为“PA-DSS 2.0到3.0变化概要”的文档，包含了标准变化有价值的信息。PA-DSS 3.0增加了一些新的要求，取消了一项旧的要求，并对其中的一些要求做了改进。为了您理解方便，这里对标准变化做一简要的总结。

增加的要求：

要求 3.4：支付应用必须限制对必需功能/资源的访问并对内置应用程序帐户执行最小权限。

应用程序安装需要确保其使用或设置了所需的权限，而没有给予额外的许可。这适用于内置帐户和服务帐户。确保你已文档化了任何缺省或服务帐户所需的权限。审核员需要验证这些文档，以验证相应的实现。

要求 5.1.5：支付应用开发人员验证整个开发过程中源码的完整性

需要确保所有的源码控制工具（例如SVN、SourceSafe、ClearCase等）被配置为仅相关开发人员能更改代码，这不排除给予某些人读的访问权限，但是需要最小化写的访问权限。

要求 5.1.6：根据安全编码技术的行业最优方法开发支付应用程序。

必须用最小特权来开发应用以确保不安全的假设不被引入到应用。为了防止攻击者获取关于应用程序故障的敏感信息，以便用来创建后续攻击。还必须确保安全应用于所有的访问和对应用的输入，以避免输入通道被破坏。这包括敏感数据和PAN在内存中怎样被处理，尝试在内存中加密这些数据与保持它在内存仅很短的一段时间。

要求 5.2.10：失效的验证和会话管理

- 将会话令牌（如 cookie）标记为“安全”
- 不要暴露 URL 中的会话ID
- 成功登录后添加适当超时和轮换会话 ID

要求 5.4：支付应用程序供应商必须将软件版本控制方法作为系统开发生命周期的一部分来进行记录和遵循。

要求 5.5：在软件开发流程中使用风险评估技术（例如，应用程序威胁建模）来识别潜在的应用程序安全设计攻击和漏洞。

要求 5.6：软件供应商必须实施流程来记录和授权应用程序和任何应用程序更新的最终发布。

要求 7.3：所有应用程序更新应包含发布说明，包括该更新的详情及影响，以及版本号的变更如何体现应用程序的更新。

要求 10.2.2：如果供应商或集成商/经销商可以对客户的支付应用程序进行远程访问，则必须使用每个客户独有的验证凭证（例如密码/口令）。

要求 13.1.1：向客户、经销商和集成商提供适用于其所使用应用程序的相关信息。

要求 14.1：每年向负责PA-DSS 的供应商工作人员提供至少一次有关信息安全和PA-DSS 的培训。

要求 14.2：向供应商工作人员分配角色和职责，包括以下各项：

- 全面负责满足 PA-DSS 的各项要求
- 与 PCI SSC《PA-DSS 计划指南》的变更情况保持同步
- 确保遵循安全编码实践
- 确保集成商/经销商接受培训并获得配套材料
- 确保所有负责 PA-DSS 的供应商工作人员（包括开发人员）接受培训

删除的需求：

要求 2.4：如果磁盘加密被使用（而不是文件加密或级别的数据库加密），逻辑访问必须单独管理以独立于本地操作系统的访问控制机制（例如，不使用本地用户帐户数据库）。解密密钥不能关联到用户帐户。

改进的需求：

要求 3.3.2：使用强效单向加密算法，基于许可标准使所有支付应用程序密码在存储期间不可读。

在应用加密算法之前，每个密码都必须组合一个唯一的输入变量。看来，加密的密码是不可接受的。在你的应用程序，你必须使用一个强的、单向加密算法（hash）与盐值。审核你的应用存储以确保您使用的是带盐的哈希算法。

要求 4.2.5：支付应用程序必须提供自动检查记录以便重建事件“通过root 权限或管理员权限对应用程序的身份识别和验证机制（包括但不限于创建新帐户、提升权限等）进行使用和更改，并对应用程序帐户进行任何更改、增加、删除。”

5. 结束语

支付应用软件在处理、传输与存储持卡人数据中扮演着非常重要的角色，PA-DSS标准为商户或收单机构在选择支付应用软件时提供了全球级别的安全评判标准，通过PA-DSS认证的支付应用软件将大大降低了商户环境中数据违背的风险，也为整个持卡人数据环境获得与维护PCI-DSS合规认证提供了保障。

参考文档和链接

[1] PA-DSS Requirement and Security Assessment Procedures Version 3.0
[2] PA-DSS Summary of changes v 2.0 to v3.0
[3] QSA Validation Requirements - PA-QSA
[4] PA-DSS Program Guide Version 3.0

艾特赛克（北京）信息技术有限公司
北京市北清路生命科学园北大科技园博雅C-Center 1号楼C座三层 102206
电话：+86 10 53056681
传真：+86 10 53056678
Email：info_cn@atsec.com