atsec NEWS
the information security provider
12/2012

最近新闻一览

更多的新闻，请参见我们的网站：
www.atsec.com

更多培训信息，请查看以下链接：
http://www.atsec-information-security.cn/cn/trainings.html

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

atsec 圆满完成 PCI DSS 2012 年底北京站培训

2012 年 10 月 20 日和 21 日，由 atsec 举办的支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standard）培训在北京，中国信息安全认证中心的培训教室成功展开。本次培训吸引了来自支付卡产业不同角色，如卡组织、银行、服务提供商、商户、卡厂，以及同行业信息安全测评机构和监管机构等 60 余名学员的高度关注。

本次培训围绕 PCI DSS v2.0 标准，内容涉及标准家族、标准委员会和产业的介绍；合规建设的思路及实施；持卡人数据环境的范围确定；网络架构和安全运维；开发安全与测试等关键内容，培训的最后，atsec PCI 实验室主任特别进行了 PCI 产业的动态分享，最新设立的特别兴趣工作组（SIG：Special Interest Group），包括第三方安全保障（Third Party Security Assurance）和维护 PCI DSS 合规最佳实践（Best Practices for Maintaining PCI DSS Compliance），atsec 将在 2013 年积极参与这两个工作组的工作并贡献自己的多年经验。之后较为详细地介绍了 2012 年 11 月风险评估 SIG 刚刚发布的 PCI DSS 风险评估指导（PCI DSS Risk Assessment Guidelines），初步介绍了 atsec 风险评估的方法论（该方法论在 2011 年度上海的 PCI DSS 培训时 atsec 有较为深入的分享，并组织进行了模拟执行风险评估的研讨会）。最后，atsec 分享了 PFI 取证调研（PFI：PCI Forensic Investigation）的方法、参考文献、流程以及结果报告样例展示。培训中贯穿主题讲演、分组研讨、案例模拟分析、有奖问答等各种丰富形式，使大家在活跃的气氛中不但学习了知识还与行业同仁们进行了有效沟通。

本期培训 atsec 特别邀请了来自卡组织的同仁分享风险管理的思路，进一步诠释了 PCI DSS 合规的重要性和必要性，同时也分享了新兴的支付技术和形态。

atsec 自 08 年以来在不同城市开展了多次信息安全领域的系列培训，为该领域的众多角色提供了一个全面的技术和经验的交流平台，并将一如既往的持续开展该领域的信息分享和技术交流。

作为持卡人，勇敢说不！

白海蔚，王长龙（atsec 中国）

据《2011 年中国信用卡产业发展蓝皮书》的信息报道：截止 2011 年末，我国信用卡新增发卡量 5500 万张，累计发卡量达到 2.85 亿张，同比增长了 24.3%；交易金额更是达到 7.56 万亿元，比 2011 年初增长了 48%。我国信用卡的交易金额在社会消费品零售总额中的占比也从 2010 年的 32.55%跃升到 41.72%。

笔者作为信用卡的粉丝自 2006 年申请使用第一张信用卡，不论国内消费还是国外旅游也的的确确感受着信用卡给日常生活带来的便利和快捷。难怪近年来信用卡红遍大江南北，已然成为上班族乃至部分学生的必要装备。更有甚者表示“一卡在手，走遍世界”。当然，如此夸张的说法无非是在炫耀信用卡相比现金、支票等其它支付方式来看，信用卡具有毋庸置疑的便利性。

不需要随身携带大量的现金，少了不法分子的关注；不用找零，少了承担沉甸甸硬币的必要；简简单单签个字即可迅速完成交易。刷卡消费的同时还可以赚取积分，兑换礼品也好还是换取航空里程也罢，都是刷卡之余的小小惊喜。如果有幸发卡行洽谈的合作商户正是你所爱，能够给个诱人的折扣，那更是让你暗自兴奋。若你临时资金周转不过来时，临时提个现也算是享受了小额免息贷款一样。如果你办的是一张外卡组织颁发的信用卡，境外消费直接按当时的汇率折算成人民币，免去了去银行排队兑换外币的麻烦，回到家也是直接人民币还款。积攒一定信用卡还款的信用值申请个人高额贷款，也让笔者在今年亲身感受了一番。这些信用卡的优势无疑在这个发展迅速的时代给大众带来更方便、更快捷、更先进的支付体验。

当然，便捷的同时风险也随之而生，自 2011 年以来，大量的数据泄漏事件的发生，使持卡人的用卡风险成为 了全球所关注的问题和隐患。而持卡人作为整个支付环节中数据的最初来源，只有所有的人都有了安全的用卡意识，才能真正的降低安全风险。下面就让我们来看看身边发生的的案例：

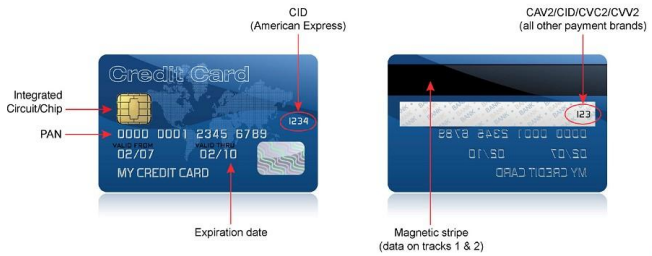
案例一：哈尔滨市民徐先生说，2009 年 10 月他收到银行寄来的催款单，说自己的信用卡透支 13000 多元，他很纳闷，自己从未办理过银行的信用卡啊。徐先生讲，2009 年 4 月，他曾经轻信办卡中介能为他的银行信用卡拓展信用卡额度，而向办卡中介提供了自己个人证件的相关复印件。但是一直也没办下来，他怀疑办卡中介利用了自己的个人信息，申请了银行的信用卡并恶意透支。

案例二：持有某股份制银行信用卡的刘先生，从来没有开通过网银，信用卡也从来没有离过身，为了保证用卡安全，刘先生不但设置了密码，而且还将卡与手机绑定，任何消费均会第一时间给予短信通知。去年 11 月，刘先生没有刷过卡，却收到银行的两条短信，说其分别刷卡消费了 4000 元。信用卡一直没离开过视线，怎么会被别人刷走 4000 元呢？刘先生立即向银行反映。银行方面核查后发现，由于刘先生的卡面信息和身份证号码泄露，有人利用这些信息在福建一票务中心盗刷 4000 元进行了电话订票的业务。

案例三：由于经常要出国出差，担心一张信用卡额度不足，今年 3 月份，广州的李女士在国有大银行申请了一张信用卡，但是几个月过去，信用卡迟迟未发下来，李女士打电话咨询时，银行方面称，因李女士在某股份制银行的信用卡存在透支未还的不良记录，所以新申请的信用卡未能获批。李女士很纳闷，自己从未与上述该银行有过业务往来，更未办过该行的信用卡，何来信用卡透支？李女士赶紧到人行广州分行查看自己的信用记录，结果发现，自己在 2009 年 6 月申办过上述股份制银行的一张信用卡，2009 年 7 月发卡的，信用额度为 6000 元。目前，存在 7161.72 元的欠款逾期未还。由于欠款预期已超几个月，该卡已经被冻结。虽然经过几番周折，最后银行方面承认有过失，自己承担损失，并向人行申请消除了李女士的不良透支记录，未给持卡人造成直接损失。

上面的案例提醒我们，只有提高个人的用卡安全意识，才能做到维护个人信息的安全，而不是在发生了安全事件后和银行、发卡机构和监督机构进行争论和推脱。另外，信用卡的离线交易只需要提供信用卡号、身份证号、信用卡的失效期和后三位码，很多在线购物网站支持这种方式完成支付。如果消费者一不小心将这些信息提交到钓鱼网站，就相当于你把身份证和信用卡给了骗子，在线购物防钓鱼是非常重要的技能。

小小一张信用卡就像是一把双刃剑，善用卡片的持卡人能够保证用卡安全，不懂用卡的人则可能成为“卡奴”甚至会成为不法分子盗刷的“工具”。怎么样才能更好、更快的提高持卡人对于卡安全的安全意识呢？先来认识一下信用卡的概念。信用卡是商业银行向个人和单位发行的，凭卡向特约单位购物、消费和向银行存取现金，具有消费信用的特制载体卡片，其形式是一张证明印有发卡银行名称、有效期、号码等内容，背面有磁条、签名条的卡片。按照发卡组织分类可大致分为：VISA 卡、万事达卡、美国运通卡、JCB 卡、Discover 卡、联合信用卡、大来卡、中国银联卡等等。



作为持卡人，我们在用卡中又有哪些需要注意的呢？

在用卡消费的过程中，最常见的也是最容易导致信息泄漏的就是刷卡凭单。目前大多数 POS 机或者 ATM 机打印出来的凭单使用的都是一种热敏纸，这种纸张上记录的字迹在一定时间周期后就会慢慢谈化直到消失。但不法分子往往不会等到字迹消失，就已经可以借助凭单上的数据去尝试进行非法的操作。针对持卡人来讲最简单的方法无非是即时销毁，比如把打印出来的卡号、有效期、姓名等相关交易信息撕碎。但随着银行、商户或者是一些终端设备厂商安全意识的提高，我们也不难发现凭单上越来越少打印完整的全卡号，更多的是采用掩码的方式对卡号进行了一定的隐藏，所以最终看到的仅仅是卡号的前六位和后四位。所以作为数据源端的持卡人来讲，如果我们再次看到全卡号的显示，不妨我们大声说“不，请对我们的信用卡信息进行保护！”

而随着互联网时代的飞速发展，网络支付和移动支付正在逐步占领市场。轻松点击鼠标，输入卡号、信用卡有效期、卡背面签名栏旁的最后三位数字，我们就可以在家里等待货品上门。在这里提出一个有关信用卡数据的概念，上右图的“123”根据不同卡组织被称为 CVV2/CAV2/CID/CVC2（以下用 CVV2 为例），CVV2 被定义为信用卡的敏感数据。从持卡人角度来讲，网络支付被认为是信用卡的几种支付方式中风险最大的一种，因为不怀好意的人可能使用网络钓鱼、窃听网络信息、假冒支付网关等手段窃取用户资料。近年来，一种被称为“快捷支付”的支付方法被持卡人使用，信用卡上所有的信息基本全部被提取记录，同时也包含 CVV2。我们充分信任商家会尽最大可能来保护我们持卡人的数据，所以充分的享受快捷带给我们的最佳用户体验。但是需要注意 CVV2 掌握着这张信用卡交易的授权，即使没有信用卡主人的同意和认可，支付的各个环节即被打开。如果我们和商户之间发生存在有疑问的交易，存储所有卡信息的商户完全可在不被持卡人同意的情况下进行扣款。所以如果某个商户在不向我们索要 CVV2 的时候就完成了交易，不妨我们大声说“不，请不要保存我们信用卡的敏感数据，更不要保存 CVV2！”

目前很多持卡人都不难发现一个问题，当我们在超市、酒店或者其他一些实体店铺刷卡消费时，收银员并不会仔细核对持卡人的签名。作为持卡人的我们试想一下，如果我的信用卡丢失且被不法分子拾到，在我没有挂失的这段时间里，如果被盗刷谁来承担这个责任呢？也许作为持卡人，我们可以联系银行对这笔交易拒付，但接下来谁又为银行埋单？银行或者商户会顺利的接受持卡人的要求吗？如果这么复杂周折的后续调查，当商户随意的处理订单签字的时候，不妨作为持卡人提醒我们的商户“不，请你仔细核对签名，也许消费者并不是卡片主人！”

也许只是点滴的积累，但需要每个持卡人自身提高安全意识。申请信用卡的时候，一定要到正规的银行网点办理，不要通过非法中介，以免你的个人资料外泄；开通网络或短信的形式，随时关注信用卡的消费情况；使用信用卡的过程中，不要把卡号留给他人，也不要把信用卡借给他人使用，防止一些不必要的损失下面笔者从持卡人角度提出一些用卡安全意识的建议：

1. 申请到信用卡后，务必在卡背面签名。在商场刷卡消费时，不要让银行卡离开视线范围；
2. 在商场刷卡消费输入密码时，应尽可能防范不法分子窥视；
3. 拿到收银员交回的签购单及卡片时，应认真核对签购单上的金额以及是否本人的卡片；
4. 刷卡消费时若发生异常情况，要妥善保管交易单据，以备对账需要；
5. 切勿签署空白信用卡账单；
6. 定期对账养成按月对账习惯；
7. 避免委托他人代办、代刷信用卡等不良用卡习惯；

8．信用卡密码及信用卡的号码、有效期、CVV2 安全验证码都不可轻易示人；

9．绑定此卡的手机，随时关注卡的支出情况；

10．如果卡不慎丢失，及时打电话口头挂失，第一时间保证卡里的资金安全；

11．每次在网络上进行交易时，不要怕麻烦重复输入信用卡的敏感信息，比如 CVV2。

只有提高了持卡人自身的安全意识，才能最好的保证自己进行的皆是安全支付，同时我们也要注意在安全标准的护卫下，我们才能更加大胆，更加放心的使用手中的卡进行消费。

支付卡行业数据安全标准 PCI DSS（Payment Card Industry Data Security Standard）是由 PCI 安全标准委员会制定，使国际上采用一致的数据安全措施。PCI DSS 对于支付网关的安全方面作出标准的要求，其中包括安全管理、策略、过程、网络体系结构、软件设计的要求的列表等，全面保障交易安全。从持卡人的角度建议其他广大持卡人在进行网络交易时尽量使用已达到 PCI DSS 合规建设的商户，以确保让安全支付过程保持最大化。

最后，呼吁持卡人要从自身的安全意识进行补充，才能更好地为信息安全支付产业做出属于自己的一份贡献，同时也为自己的用卡消费带来最大的安全保障。

atsec 2012 年部分 PCI 成功案例展示

2012-01 atsec 完成安利中国的 PCI DSS 合规性评估
http://www.atsec-information-security.cn/cn/news--277.html

2012-01 atsec 完成盛付通 PCI DSS 符合性评估
http://www.atsec-information-security.cn/cn/news--279.html

2012-08 atsec 中国完成 Securespay PCI DSS 合规性评估
http://www.atsec-information-security.cn/cn/news--300.html

2012-10 atsec 完成民生银行信用卡中心 PCI DSS 符合性评估
http://www.atsec-information-security.cn/cn/news--304.html

2012-11 atsec 中国完成 Ecward PCI DSS 合规性评估
http://www.atsec-information-security.cn/cn/news--311.html

2012-11 atsec 中国完成 VimaPay PCI DSS 合规性评估
http://www.atsec-information-security.cn/cn/news--312.html

2012-12 atsec 中国完成中银金融商务昆山分公司 PCI DSS 合规性评估
http://www.atsec-information-security.cn/cn/news--314.html

恭祝所有atsec客户、合作伙伴和全体员工新年快乐，万事如意

感受第十三届巴黎召开的国际 CC 会议

atsec，白海蔚

2012 年 9 月 18 日至 9 月 20 日，第十三届 2012 年度国际通用评估准则会议（ICCC：International Common Criteria Conference）在浪漫的法国巴黎召开。这是法国第一次举办 ICCC 会议，也将法国人独有的热情注入到了 CC 标准产业这个信息安全技术性较强的领域。

atsec作为全球信息安全领域的领导者共有十余名顾问参加了本届CC大会，多篇专业论文在本次会议上发表演讲且被高度关注。其中，atsec中国总经理刘岩在本次ICCC会议上发表了题为“移动支付安全方案（Security proposal on mobile payment）”的主题讲演。他本人也受邀参加大会开幕式的圆桌会议讨论（Panel Discussion）环节，与其它四位国际信息安全领域的专家共同探讨“移动和安全”。笔者作为atsec的一员深感自豪，并且借助CC大会这样的平台在信息安全行业与其他安全专家交流亦是非常难得的机会。

图：部分 atsec 成员在 13ICCC 的合影

本届 CC 会议的开幕式上，大家一同怀念了 2012 年初离世的德国 BSI 同事 Irmela Ruhrmann 女士，她为 CC 的发展做出了巨大的贡献。

会议自第一天主题讲演和开幕式之后，共设有 3 个分会场，分别探讨不同类型的话题，比如体系更新、来自 CC 社区的报告、CC 和新技术、加密、移动安全、安全开发、虚拟化、CC 和其他标准，以及相关的经验分享等等。笔者在为期 3 天的会议过程中针对感兴趣的议题进行了学习和积极参与，本文简要阐述笔者经历本届 ICCC 的一些感受。

移动安全引发的关注

移动安全（Mobile Security）问题是本届 CC 会议最为关注且重要的议题。

会议的关键主题（Keynote）讲演阶段，两篇分别来自 GIE-CB 和爱立信（Ericsson）的演讲都不约而同的谈及了移动安全的问题。CB 作为来自支付产业典型的 CC 消费者（Consumer）也即厂商的最终用户，分享了引入 CC 标准提高信息安全的经验，并提出了期望和新的调整计划。当谈及信息安全评估和认证时，还分享了 CB 相关安全认证的历史：1996 年通过首个 ITSEC 认证；1999 年获得了第一个 CC 认证；2001 年获得了高级别的 CC 认证。此外诸多的信息安全标准也是 CB 安全评估和认证的重要参考，比如 ANSSI、PTS、支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standard）和支付应用数据安全标准（PA DSS：Payment Application Data Security Standard），目前正在致力于 PCI 和 CC 标准的融合以及评估结果的互认，以便最大限度完善安全评估和认证的框架。同时，来自移动领域新的挑战也被提出，并期待着业界同仁们深入的探讨。如远程移动支付、近距离支付、可信的执行环境（TEE：Trusted Execution Environment）、点对点加密等。以及 PA DSS 可以作为软件评估的重要安全基础，这也是 atsec 刘岩在其后面的主题讲演中提到的类似观点。来自爱立信的主题讲演则是作为通讯行业 CC 消费者角色的重要代表，其讲演的题目是“使用 CC 作为移动网络安全保障方法论”。讲演中介绍了 3GPP 安全保障，3GPP 保护轮廓（Protection Profiles）也正在进行制定完善，并将被提交进行 CCRA 的审核，其大体包括 HSS PP、RBS PP 和 SGSN PP。为了实现基于 3GPP 网络功能的产品和信息安全保障的稳定，3GPP 和 CCRA 紧密工作，共同探讨并就工作范围达成一致，深入 3GPP 和 CCRA 相关的制定流程和方法论。可以看到上面两个典型 CC 产业的用户角色，都积极参与到从用户角度针对不同标准进行产业之间的整合工作，使得 CC 标准的使用范围更加广泛，效果更加充分。

关键主题结束后，六位受邀专家以圆桌会议讨论（Panel discussion）的形式共同探讨了“移动安全”这个新兴却备受关注的安全话题。各位专家探讨了如何应对移动安全的新威胁，由于这些安全威胁带来的较新的安全保

障需要被要求和提出，各位均表示应用 CC 标准提供在移动安全领域的保障是可行的。而整合不同的认证体系满足市场要求将是推动 CC 更加健康良性发展的有效方式，比如在移动支付的特定领域和 PCI 产业的协同工作。

本届 CC 会议采纳并录用了诸多的谈论移动安全，特别是移动支付相关的安全主题讲演，包括 Smartphone Applications - Common Criteria is going Mobile、(U)SIM certification process: configuration issues、Security requirements for NFC devices、Vulnerability Test for Mobile Device Management System。atsec 中国刘岩讲演的题目是“移动支付安全解决方案（Security proposal on mobile payment）”，讲演提出了一系列的关于移动支付的安全解决方案，以应对移动支付的安全威胁。方案涉及三个级别：环境和物理安全、支付应用安全，和组织安全，同时方案也初步探讨了如何将 CC 标准和支付安全 PCI 产业标准相结合，从而最大限度提高标准整合和结果的适用性，比如支付应用 PA DSS 标准则可以引入作为支付应用的保护轮廓 PP 等等。

图：atsec主题讲演

体系变化和 EAL 级别的接受

CC 会议特别安排了一个分会场来讲解各国家 CC 体系的变化。多年来，美国体系以独树一帜的策略要求也或多或少的影响着 CC 产业发展的方向。美国体系已经降低了评估可以接受的最高 EAL 级别为 EAL 2 级，可以说 EAL 3 或者更高级别的 CC 认证在美国是不太可能的。而理论上存在的可能性是可以在其他国家进行 EAL 4 级别的 CC 认证，然后将其引入到美国体系，但是经常会遇到一些技术细节的干扰。比如因为增强的要求、PP 中定义的特定保障活动、FIPS 140 要求或者 AVA_VAN.5 等，技术上来讲已经被美国确认在 CC 互认范围之外。该思路将国家安全和 CCRA 互认的产品安全相区别，然而无形中在 CC 技术领域被诸多的专家和顾问认为是 CC 产业技术的倒退，因为 EAL2 级别的评估技术角度来讲比较初级，不需要完整的安全设计审查，不需要源代码审核，甚至脆弱性分析也比较初步。故而两年以来，该调整和趋势在产业内也引发了较大的争论。

CCRA管理委员会（CCMC：CCRA Management Committee）已经就关于CC应用和CCRA发展趋势的远景声明（Vision Statement）达成一致，并在CC官方网站上发布，参见：http://www.commoncriteriaportal.org/vision.cfm。其涉及的关键内容如下：

- 通用的 ICT COTS 认证产品的安全级别需要被提出，做到不严重影响这些产品的价格和可用时间。
- 为了支持上述目标，标准化的级别通过建立技术社区（TC：Technical Community）开发协同保护轮廓（cPP：Collaborative Protection Profile）和支持文档（supporting document）得到提高，实现更加合理化、可对比、可重复且成本划算的评估结果。
- 互认应该基于 cPP 所规定的通用级别。
- 针对所有产品类别的 TC 和 cPP 应该得到定义，使得厂商针对同类产品提供其个体的安全目标（ST：Security Target）。
- 如果可能，cPP 应该尽可能的替代个体的 ST 进行安全评估。ST 的应用将专注在 cPP 不存在或者不可用的情况，且 CCRA 互认应限定在 EAL 2 级别。
- CC 将作为工具箱被维护，用于 TC 开发 cPP。
- 高于 cPP 规定的评估级别应在如下条件下保留采用：国家要求；个体参与者的认可，如国家、COGIS-MRA 和类似的其他社区的认可；高于 cPP 级别没有 CCRA 互认可以采用。
- 保护轮廓（cPP）和/或支持文档将涵盖脆弱性分析的要求，确保认证的产品实现预期的安全级别。

以上观点在 2012 年 9 月 17 日的 CCMC 会议上得到分享，所有国家均表示同意 cPP 的概念，以及基于 cPP 的方法可以协助实现可重复、可比较以及有效的评估结果。两个国家表示不赞成限定非 cPP 互认到 EAL2 级别。故而，额外的讨论将由 CCRA MC 召集并将努力达成一致。执行工作组将受任进一步完成细致的工作方案，包括更新的 CCRA 互认协定和转换计划等，并计划于 2013 年第一季度的 MC 会议上呈现。

笔者也看到，上述调整趋势在CC产业引发了一些争论。总之希望这些沟通和争议能够促进CC产业的发展，在保护国家政策的基础上，平衡贸易和商业互认要求，保障来自用户的信息安全考虑，使得调整和改变能够确保CC评估结果的质量和标准的良性发展。

证书颁发

本届 ICCC 会议的证书颁发环节依然安排在第二天晚上的 Gala Dinner，与往届略有不同的是本届 Gala Dinner 采用了较为放松的社交方式，大家可以自由走动，彼此交流。

证书颁发环节按照不同的认证机构分别展开。其中，atsec的长期合作伙伴IBM在法国巴黎的第十三届国际通用评估准则大会上获得了四个面向其复杂的IT产品的通用评估准则证书。获得的证书为：

- z/OS Version 1 Release 13
- DB2 Version 9.1 for z/OS Version 1 Release 10
- AIX 7 for POWER
- PR/SM on IBM Systems z196 GA2, z114 GA1

所有这些产品都已通过了最高商业级别的(EAL4+)评估。在这个最新的颁奖典礼上，atsec 再次展示了她是最高保障级别复杂和创新评估的首选实验室。

CCRA 动态分享

自从 2011 年度马来西亚的 ICCC 会议以来，CCRA 成员国家没有发生变化。2012 年 CCRA 分别针对西班牙、挪威和韩国国家体系执行了 VPA/Shadowing，并计划于 2013 年执行土耳其、意大利、瑞典，以及其他两个新的即将成为认证颁发国家的体系执行 VPA。

今年 9 月份，通用评估准则用户论坛（CCUF：Common Criteria User Forum）的建立在巴黎通过 CCMC 的认可，且鼓励更多的参与者加入到 CCUF 行列。笔者在此也呼吁更多的中国的机构加入到 CCUF，更多信息参见链接：http://www.ccusersforum.org/。来自 Mme Alicia 的主题讲演 CC Users Forum Report to the Community 进一步较为详细汇报了 CCUF 的工作情况和发展，得到了来自各方的参与和讨论。来自 atsec 的专家也提出建议，期望更多的来自亚洲的用户加入到 CCUF 甚至参与到管理和运营工作。

目前，CCMC 的主席是来自瑞典的 Dag Stroman（任期一年），ES 主席为来自美国的 Mark Loepker（任期两年），DB 主席为来自英国的 David Martin（任期两年）。

本届会议统计和下届展望

本届 CC 会议吸引了来自 27 个国家共 385 位代表参加，其中法国 104 名、美国 64 名、德国 45 名、瑞典 9 名，中国虽然尚不是 CCRA 互认国家，也有约 40 名行业专家出席了本届会议。由此不难看出，来自全球不同国家的信息安全专家对 CC 产业给予了高度且持续的关注。

大会的最后宣布下届 ICCC 会议将于 2013 年 9 月份在美国举办。让我们共同期待吧！

更多信息可以参见如下链接：

atsec 网站：http://www.atsec.com/us/news-iccc-2012-271.html

13 届 ICCC 官方网站：http://www.iccc2012paris.com/

CC 官方网站信息：http://www.commoncriteriaportal.org/iccc/