停车坐爱枫林晚

- 感受 2021 年度 PCI GCF

atsec 刘岩，2021 年 10 月

老舍先生说：“秋天一定要住北平”。北京的秋是铺满金黄的银杏叶小路，是漫山遍野的红叶所点缀的山岭沟堑，同时也是收获的季节。这个深秋的周末，驻足于北京城一个安静的咖啡厅。它所吸引我的不仅仅是秋色环绕的美景和用心的布置，也包括里面的人们，有学生们在复习功课，有年轻的朋友在探讨创业的想法，有的正在忙碌创作于自己的幻灯胶片，也有的发呆享受宁静的下午。而我，在三天支付卡产业全球社区论坛结束之后，还可以戴上耳机独自慢慢倾听来自于产业各位专家的讲座，这也未尝不是件惬意的事情。

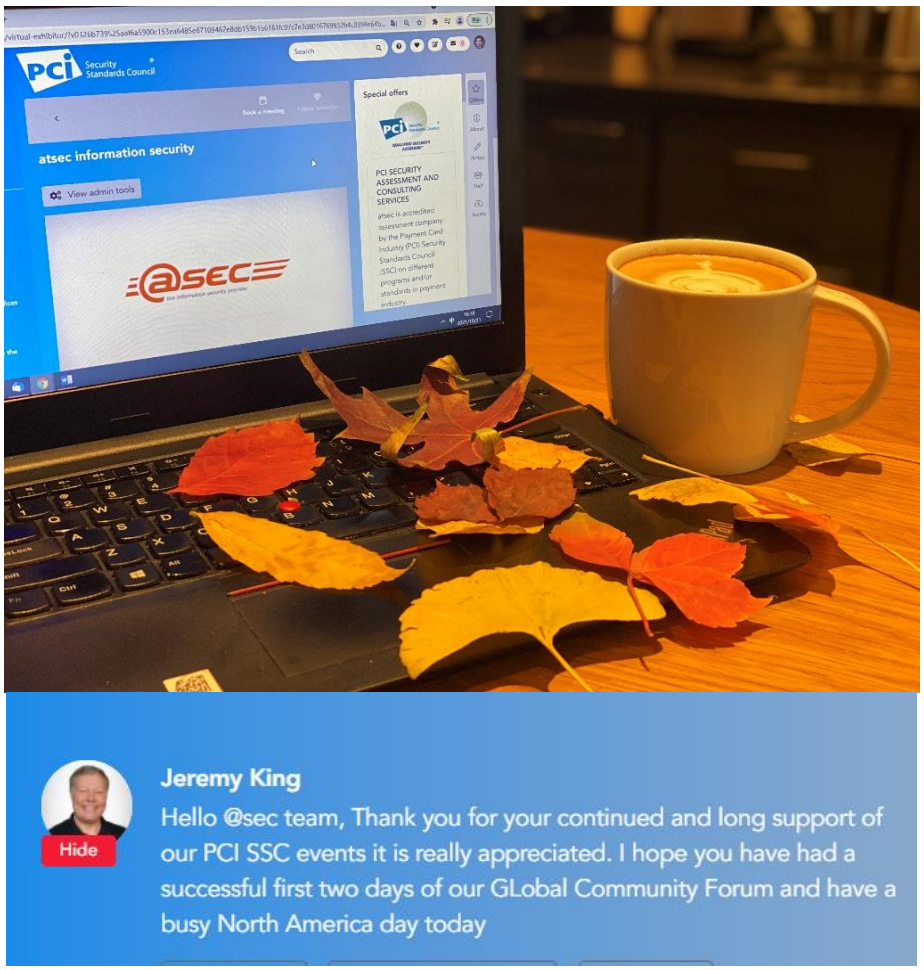
回想这十几年来，每年的 10 月和 11 月份 PCI 产业会组织不同区域的各种会议，大家奔波于各个国家和城市，分享交流，乐此不疲。时光荏苒，像 Bob、Gill、Ralph 这些老朋友也依次或即将退休，但我们仍旧感恩于他们对产业做出的贡献；而同时也结识了很多新的朋友，为这个产业带来了新的想法、产品、技术和热情。2020 年初以来，这个世界进入到了比较特殊的时期，大家都减少了差旅的奔波；而人类真是非常适应变化的群体，面对面的交流受到了限制却似乎没有减少产业的各种沟通，甚至有些加强……在线的各类平台、不同形式的产品满足着不同的会议需求。就以全球的支付方式来看，和中国的情况类似，线上的非接触支付类型由于疫情得到了飞速的发展，比如在日本、巴西、印度等等各个国家的无现金支付、二维码支付等都在这段时期内得到了更加广泛的采用。不知道这样的形式未来还需要持续多久，但是我相信 2020 年初所出现的全球疫情对于人的影响不仅仅是健康层面的，还有整个社交方式的改变所带来的感受。

按照往年的计划，这个时间或许在会场展转于各种产业交流、或许在准备各个或大或小的会议发言、或许正在和来自世界各地的这一年内难得见面的新老朋友们喝着咖啡或啤酒闲聊，亦或是会后一起到诺坎普看一场足球赛……而这一切似乎有了变化，但又似乎因为在线技术的成熟并没有让我们的交流受到任何的影响，就像 Lance 提到 PCI 产业这一年 PCI DSS 4.0、SSF 标准 Module B 的发布等重要工作都如期进行着。而另一方面大家也表达着不能面对面交流的遗憾，Troy 在他的主题发言中增加了一些西式幽默的过渡环节，比如隔着屏幕和同事递上红酒杯，用游泳圈设想海边休闲……这些其实我是能感同身受的。

今年七月份的时候，Troy 找到我谈及希望在 PCI GCF 上讲个话题，邀请这个产业不同角色，采用不同的语言，从不同的维度谈一谈**这个世界“断开”的时候我们的使命还在继续**，而 atsec 和我本人所参与的全球执行评估机构圆桌会议 GEAR 恰好作为评估机构的代表针对远程评估、高质量审核等有过诸多的探讨，而我也和 atsec 从事其他标准评估的同事有过诸多探讨，比如 CC、FIPS 140、GSMA 等，这种部分远程配合更专注的现场工作的混合型审核方法，也是这段时间在评估产业不错的积累。我很高兴看到 Troy 所组织的主题讲演话题引入了诸多的产业同仁共同参与，他们分别来自 PCI SSC、Target、Australian Payments Network、Cloud Security Alliance 等，谈及了标准发展、密码、远程审核、云安全等等诸多重要的话题。由于大家在思路上的相互理解和默契，基本上我们只是经过一次几分钟的彩排就对要演讲的话题具体内容达成了一致。

上图为 Troy 所组织的主题讲演的议题简介

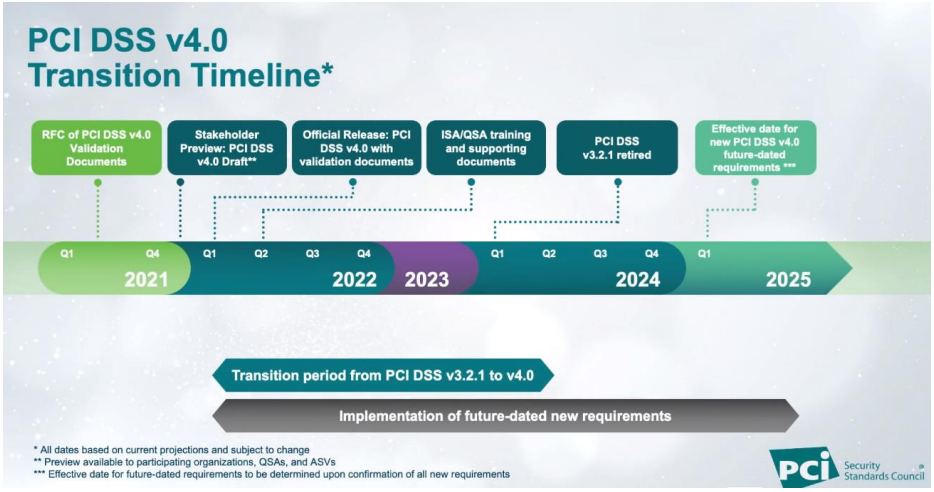
atsec 也持续多年成为了**会议的参展商**，和产业分享着我们最新的经验和相关服务，与数百名参会专家一起积极的就技术问题进行沟通和探讨。



上图为 atsec 在 2021 年 PCI GCF 的虚拟展位首页

除了 PCI 产业完整的标准领域审核服务以外，我们也介绍了 atsec 在其他标准领域的积累，比如 Common Criteria、FIPS 140、GSMA、O-TTPS、ISO/IEC 27001 等等。这些标准都是相辅相成且互相促进的。

PCI DSS 标准的最新版本 v4.0，应该是目前产业最为关注的话题。原因也很明显，PCI DSS 标准在这个产业的历史最为悠久，而发挥的作用也是显而易见的。PCI DSS 计划保留了原有的补偿控制措施，并引入定制化的方法，使得标准的适用性更加广泛、更加灵活。



上图为 PCI DSS v4.0 过渡的里程碑计划（原图来自 PCI SSC）

总体来讲我们可以看到新版本标准还在紧锣密鼓的审核和最终发布阶段，标准和相关验证文档计划 2022 年 Q1 发布。经过大约两年的过渡期，2024 年 Q1 老版本标准 PCI DSS v3.2.1 将退出历史舞台。在 atsec，我和我的同事也从很早就开始关注 PCI DSS v4.0 的变化，投入了一定的标准开发和反馈的工作，相信我们会协助所有的被评估结构平稳的过渡到新标准。在此过程中我们也期待着更多的交流和沟通。

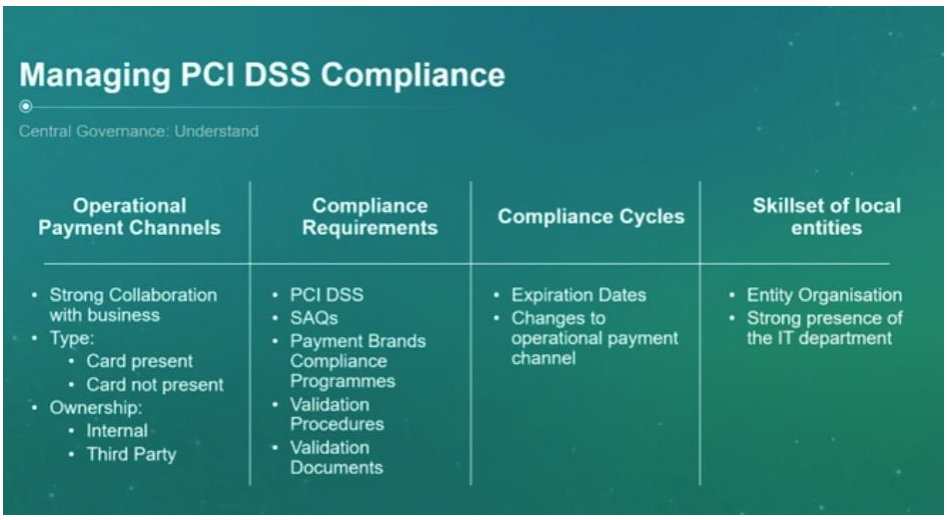
另一个值得提及的重要标准和体系是 **PCI SSF，也即软件安全框架**。这个体系下的软件安全标准替代了之前的 PA DSS 标准，也在近期发布了软件安全标准的 Module B – 终端软件安全，未来这个标准会有更多的 Module 持续发布，从而适应更加创新的支付软件领域。本次会议有多个关于 PA DSS 向 SSF 迁移的话题讨论。包括 PCI SSC 和产业专家共同发表了关于“采用 SSF 降低电子商务中的普遍风险”的讲演，以及“PA-DSS 之后的生活：机构从 PA-DSS 向 SSF 迁移的重要考虑”。我们知道 PA DSS 源自最早 VISA 组织于 2005 年发布的 PABP 体系，而 PA-DSS 更适合传统的支付方式，目前已经不再适应新的支付软件的形态（如移动支付）和开发模式（如敏捷开发）等。SSF 体系分为两个独立的标准和合规评估体系，一个是软件安全标准，一个是安全软件生命周期标准。安全软件的实施引入了基于目标的风险评估方法，更加适应未来的快速发展以及更加广泛的支付软件形态，支持更多的软件类型、架构和开发方法。SSF 标准最早发布于 2019 年初，并于 2021 年第二季度进一步更新完善。关于 SSF，可以参考我的同事张力刚刚发表的一篇技术性介绍文章，谈及了“PA DSS 到 PCI SSF 标准的过渡”。

信用卡卡号涉及的 **8 位 BIN** 也是近期较受关注的变化，PCI SSC 发布了相关指导和 FAQ 1091，大家也可以参考。本次会议也多次提及了涉及八位 BIN 转变的探讨，如题为“8 位 BIN 的迁移 – 范式化转换！破坏性的变化？”的技术讲座，和大家就探讨了 8 位 BIN 转变过程中的重点和难点。与此同时，atsec 我的同事李迪也编写了一篇中文的文章“8 位长度银行卡 BIN 码在 PCI DSS 中的实践”，可以参考。

密码学是信息安全领域的基础，而 PCI 标准家族中的诸多标准与密码算法和密钥管理有着紧密的联系，特别是 PIN、P2PE。本次会议也收录了针对密码领域的话题分享，比如针对 ISO Format 4 的 PIN block 向 AES 迁移的技术考虑和最佳实践分享、不同标准中的加密设备管理，以及多租户硬件的 HSM 安全要求（这些要求也会即将加入到最新的 HSM v4.0 标准中）。而说到这里，就不得不提及国际密码模块会议（ICMC：Internatioanl Cryptographic Module Conference），该会议是由 atsec 所发起的，每年度的盛会整合了产业不同角色机构的积极参与，包括认证机构、厂商、密码学研究机构、测评机构，当然也包括重要的标准化组织如 PCI SSC。来自 PCI SSC 的 Troy 和 Ralph 都在 ICMC 会议上发表技术分享，做出了积极的贡献，不同标准之间合作和互通为整个技术产业呈现了积极的结果。

图为本届 PCI 会议上 Troy 谈及 Ralph 在密码领域对 PCI 以及 ICMC 的贡献

“**大型零售商如何为所有子公司管理其 PCI DSS 合规**”，我个人认为这个分享非常值得学习，来自 Schwarz IT KG 的支付安全总监分享了作为大型商户 Lidl 如何持续高质量的进行 PCI DSS 合规的。Lidl 是主要分布在欧洲的大型超市，拥有分布于 33 个国家的多于 12500 个商店。我在欧洲生活或旅游期间对其物美价廉印象深刻，而对于安全合规的重视也是体现了德国企业各个层面严谨的态度，我想这也正是品牌长久发展的根基。



上图来自 Lidl 关于 PCI DSS 合规的分享

Lidl 将业务、支付安全和 IT 做了有机的结合。Lidl Pay 系统的最佳实践应用了 P2PE 解决方案，安全合规工作采用了自身内审和 QSA 配合的方式。Lidl 也将 PCI DSS 的合规和 ISO/IEC 27001 信息安全管理体系（ISMS）做了整合，还关注于整合新的技术和支付方式，如云安全领域，从而更加灵活且高质量的应对变化和革新。随着每年度产业的变化、标准的变化、自身的技术架构调整等等，积极做好 QSA 评估的准备，追求第三方审核的高质量以及中立性，而不仅仅是认证的结果。

上图来自 Lidl 关于 PCI DSS 合规的分享

此外，会议还有针对全球**数据泄露以及漏洞趋势**的探讨和分享。比如来自 MIT 分享的“全球数据泄露数据库和挑战”，通过不同年度数据展示了不同地区、不同类型数据泄露事件的宏观情况，并进行了必要的分析。渗透测试领域的专家也分享了其研究的成果以及一些漏洞挖掘的经验，从攻防的角度做了生趣的讲解。

写着、听着……咖啡凉了，天也黑了，深秋的北京天高云淡，显出了淡淡的寒意，而大家对于参与会议的热度还经久未尽。希望这个世界的技术交流很快可以更好的连接起来。