2023 高交会商密展团零信展位密码讲堂-商密证书透明、商密证书自动化

大家好！

今天高交会最后一天，我们坚持按照原来的讲座安排把最后一讲讲完。

今天讲证书透明和证书自动化，正好，刚刚收到一个与证书自动化有关的喜讯，插播一个喜讯。我们刚刚拿到这个高交会组委会颁发的“优秀产品奖证书”这个获奖产品就是国密 HTTPS 加密自动化网关，这个正好跟我们今天讲的自动化有关系，所以插播一下这个。

那我们就开始讲什么是证书透明？为什么需要证书透明？今天会讲这几个方面的内容，第二，证书透明机制如何保障 SSL 证书的安全？第三，什么是商密证书透明？我们把采用商密算法实现的证书透明叫商密证书透明，那么，采用国际算法的证书透明就叫国际证书透明。为什么我国急需证书透明，还会介绍一下《证书透明规范》这个正在立项制定的商密标准，零信技术牵头制定的一个国密标准。再介绍一下使用情况和生态情况。

那什么是证书透明？为了保证 SSL 证书的安全，浏览器只信任通过严格认证的 CA 机构的根证书签发的 SSL 证书，但是，如果这个浏览器信任的 CA 系统被恶意签发了不该签发的证书，或者 CA 系统被攻击了，或者 CA 操作失误，错误签发了 SSL 证书，怎么办？如何能够及时发现错误签发或者恶意签发的 SSL 证书，这就是证书透明的用途。大家看看证书透明官网上写的很清楚，Working together to detect maliciously or mistakenly issued certificates，大家协同工作检测恶意签发或者错误签发的证书，这就是证书透明的目的。就是为了解决这个目的，谷歌发明了这种证书透明，叫 CT，Certificate Transparency。这个名字取得很高大上，透明，大家

都知道管理透明。其实就是一个证书备案系统，跟我国的网站备案一样，网站要备案，签发证书也要备案，你签发证书之前先到证书备案系统去备案，备案完才能给用户。就是说，这张证书一旦备案了，还没有给用户部署之前，大家能知道这张证书是应该签发还是不该签发的，所以，这个机制非常好，透明公示，这个机制非常好！

为什么好？打个比方，相当于这个出生证，孩子没出生之前你必须先办好出生证，并且这个出生证要放在证书里面，SSL 证书国际标准增加了一个字段，SCT 列表字段，专用于必须把这出生证放到证书里面，随时备查。谁查？浏览器查。随时备查，你每天必须把出生证揣在兜里。如果没有这张出生证，这张证书是不信任的，浏览器不信任，等会给大家演示一下，浏览器怎么不信任，没有出生证不信任。所以，这个是一个很好的监督机制。既监督了，还高大上！所以，为什么全球 CA 都响应了,因为你签发行为都不敢公示，说明你是想搞什么鬼，大家都不愿意背这个锅。这是一个高大上的道德高地，这是第一招。

第二招，由于谷歌浏览器市场份额已占到 70%以上，如果你签发的证书没有到我这里来备案，没有拿到准生证，没有把这个出生证放在兜里随时被查，浏览器就不信任你，根预置了也没有用，这一招太厉害了。这是有事后监管和事前审查，符合我们的管理理念，事前，你要做认证，把你的根做我的预置，要做审计，说明你是你是规范操作的 CA，事后发证书过程我都会监管，怎么监管？我也没法查你，没法去你公司查你。全世界有人查你，只要签发证书进了数据库，随时可以查你，因为很多第三方服务提供订阅服务，我的域名有没有被哪个 CA 机构恶意签发了证书，随时提醒你，你只要证明这个域名是你的，就会提醒你。所以，它是会有实际的好处，就是透明，为什么叫透明，你想干坏事就干不了，不敢干！所以，这是一个很好的发明，一种监督方式，这个方式能保证证书的本身的安全。

因为 SSL 证书太重要，它保证互联网的基础通信安全，我上次讲过 SSL 证书自己的安全怎么办，证书透明来监督它。这是昨晚数据，从 2013 年开始，有证书透明开始，全球信任的 CA 签发的证书已经有 110 亿张了，同志们，110 亿张 SSL 证书全部实现了证书透明。这个当然与谷歌的垄断地位有关系，有两个层次，一个是道德层次，这个规范约束的层次，为什么需要证书透明，就是为了防止恶意签发或错误签发。因为谷歌他是恶意签发的受害者，绑定谷歌域名证书，被恶意签发，他没办法，就搞了这个证书透明。

这是一个生态系统，整个生态的各方都支持的一个系统，当然，首先是必须证书透明日志系统，你要我备案，得有地方去被备案，必须有先有备案系统，正式名称叫证书透明日志系统，log 系统。这个日志系统是谷歌是自己开发的，并且完全开源了，大家都可以，鼓励大家都可以运营这个日志系统，当然，必须通过谷歌的严格审查，目前全球有除了谷歌以外还有其他五家也运营自己的 CT 系统，这些 CT 系统预置到谷歌浏览器信任就可以用于验证 CT 数据了。

这是第一个生态成员，首先必须有证书透明日志系统。

第二个生态成员是 CA 机构，CA 机构发证书必须去备案，把 CT 数据嵌入到证书里面去。谷歌当然也是一个参与者，Google Trust 现在全球排名第二，所有浏览器信任的 CA 都要支持 CT，都升级改造 CA 系统，因为 SSL 证书要加一个字段进去，所以需要升级改造。

第三生态成员是浏览器，浏览器当然也要支持，要查验 CT，CT 里面多了个字段，不分析不行。很有意思，火弧浏览器不支持，我觉得很有意思，这里面能看到火狐浏览器已经跌到第五位去了，因为你都不查 CT，我觉得是不可信的浏览器，所以，火狐浏览器的份额很小了，才百分之三了。

第四个生态成员就是监督审计方，CT 是全世界公开数据库，有很多公司做数据分析，分析有多少 DV/OV/EV 证书等。我们发的每个季度的 SSL 证书市场简报里面数据都是引用 CT 数据。另外，有像 Facebook 还提供服务的，可以通过社交媒体通知你，谁给你签发了 SSL 证书，让你马上知道。

这是一个生态，没有这个生态是实现不了闭环的。而这个 CT 系统里面为什么要有 6 家 CT 服务提供商？谷歌的 CT 政策是这样的，一年有效期证书必须提交 3 个 CT，什么意思？CT 是分布式架构，必须有多家提供 CT 服务，如果只有一家 CT，那提供不了服务怎么办？所以，一般都是提交三四个 CT，返回数据后你写进三个。有效期为一年的证书必须要有 3 个 CT 数据，180 天以内证书必须有两个 CT 数据。谷歌以前政策是 3 个或者两个里面有一个必须是谷歌 CT，其他可以是其他家 CT，这个很有意思，必须有一个。但政策现在改了一下，可以没有谷歌 CT，可以其他 3 个家 CT，但实际上大家都还用谷歌 CT，为什么？因为我的业务系统就这么做了，我还会改吗？不可能再改了。

我们看一下 CT 是什么东西，看一下 CT 在谷歌浏览器里面什么样的，谷歌浏览器证书查看器能看到 SCT 列表字段，它翻译成：签名证书时间戳列表，翻译不对，应该是证书透明日志数据列表，它没有做解析。里面 CT 数据就是乱码，在谷歌浏览器证书查看器看。但是，你把证书存下来以后，用 Windows 证书查看器看，Windows 解析了里面有个字段叫 SCT 列表，里面有三家 CT 数据，Windows 把 CT 数据给解析出来，第一个是版本号，有 CT 日志 ID，还有 CT 签名时间，用什么算法，SHA256,ECDSA，用 ECC 算法，还有 CT 签名数据，Windows 证书查看器展示了各种 CT 签名数据。这是谷歌浏览器和 Windows 的展示效果。

如果没有 CT，浏览器怎么显示？先用谷歌浏览器看一下，大家可以自己体验一下，访问 https://no-sct.badssl.com ，这张证书里面就没有 CT 数据，谷歌浏览器会显示：Err_Certificate_Transparency_Required，需要 CT，没有 CT 谷歌浏览器是不信任的，有警告，不信任！没有 CT 的国际 SSL 证书不信任，这是目前国际 CT 的情况。

我们国家是不是需要商密证书透明？目前没有，全世界所有国际 SSL 证书都有 CT，我们是不是应该也有？也应该采用这样机制来保障商密 SSL 证书自己的安全，对不对？这个道理很简单。所以，我们就牵头制定了一个标准，这个商密标准在后面会讲一下。

商密 CT 就是把里面的密码算法换成商密 SM2 签名算法，哈希算法换成 SM3，这样商密 CA 就可以提交 CT 日志系统了。你用谷歌的 CT 提交不了，谷歌 CT 用 ECC 算法的，谷歌 CT 也不信任国密根证书，不支持国密算法。CT 系统是只允许其信任根签发的证书才能提交 CT 日志系统，不信任的当然提交不了。所以，我们没法用国外的、美国谷歌运营的 CT 系统。我们必须有自己的 CT 系统，因为 CT 签名算法也要变成商密的，SSL 证书也要支持商密 SSL 证书。这个机制是一个非常好的机制，我们必须要用它来保障我国商密 SSL 证书的安全。

所以，我们就打造了一个商密证书透明 CT 系统。刚才讲了国际 CT 生态是什么样的，我们也是需要有一个四方参与的生态，我们是在去年世界互联网大会发布的这个生态，因为必须先从证书透明开始，我们今年在高交会发布的是证书自动化，连续打造了两个生态。这个生态里面必须有国密证书透明日志系统，没有日志系统，就没有地方提交证书。所以，我们研发国密日志系统，是基于谷歌开源的日志系统，把算法全部换成商密，支持商密 SSL 证书，支持商密验证。我们也开发了一个国密 CA 系统，能够签发商密 SSL 证书，支持商密证书透明的商密 SSL 证书，因为如果我们只是搞一个证书透明日志系统，要求 CA 机构都来支持国密 CT，不会有人响应。现在有响应了，有七八家 CA 响应的。所以，还不如我自己干了 CA 系统能签发支持证书透明的证书，我自己提交了国密证书支持国密 CT，来验证打造的生态。目的是为了验证这套系统是否可行，能不能走通，把 CT 系统从国际算法换成商密算法行不行。所以，国密 CT 日志和国密 CA 系统这两块我们都自己做了。

光有这两块还不行，还需要浏览器支持，因为证书里面有商密 CT 数据，没有浏览器支持不行。但是，现有的国密浏览器都不支持，怎么办？所以，我们就做一个国密浏览器，零信浏览器，零信浏览器第一个支持国密 CT，预置信任国密 CT 日志系统，就能够验证国密 SSL 证书里面的国密 CT 信息，CT 签名信息，能够都展示出来。至于第三方，监督审计方，我们 CT 系统目前有两三万张国密 SSL 证书，第三方机构可以查库。

我们目前运营了三个正式 CT 和一个测试 CT，只要是零信浏览器信任的国密 CA 机构都可以免费使用，免费提交获得 CT 数据，透明公示，零信浏览器信任。零信浏览器怎样展示 CT 呢？这也有创新，来看一下，这是高交会官网，看看我们浏览器如何展示证书透明，国际 SSL 证书已经每一张证书都支持证书透明，我刚才给大家看过谷歌浏览器怎么支持的，就显示一堆乱码，而 Windows 把它解析出来，但是 CT 日志 ID 也是一串数字，零信浏览器的创新在哪里？看看高交会网站这张证书，点开加密锁，原来浏览器只有 连接已加密，证书有效，我们在下

面加了一个证书透明的菜单，展示这张证书里面有三个证书透明日志数据，算法是 ECC，哪三个 CT？我们会展示，谷歌 Argon2024, DigiCert Yeti2024，Cloudflare Nimbus2024，里面有三个 CT 都给它展示出来了，我们说，零信浏览器全球独家透明展示证书透明，什么意思？有证书透明，证书公证过了，公示了，但是用户不知道你公示没有，零信浏览器给你展示出来，不仅告诉你公示过了，而且告诉你在哪家 CT 系统公示的，还再告诉你在哪个 CT 服务器公示的。这是一个很好的创新，让证书透明更加透明，一清二楚！

这是国际 SSL 证书，我们独家支持的，其他浏览器没有这个功能，他们只是显示有这个 SCT 列表字段而已。那国密证书怎么展示呢？也一样，显示 证书透明(SM2,3)，哪三个 CT 也会展示出来给你看，目前只有我们运营的三个 CT 系统，我们签发的国密证书都提交这三个国密 CT 系统了，目前也只有零信技术两个国密 CT，证签技术 SM2CT2024,零信两个，一个是 SM2CTcom2024，一个是 SM2CTcn2024，3 个 CT 网址全部都提交，看一下，有 3 个，这个也是我们的一个创新，透明展示证书透明！

国际证书透明有没有？有，给你透明展示出来。国密证书透明有没有？有，也给你展示出来。如果没有的话，显示：证书不透明，红字。目前是这样的处理的，不是像谷歌浏览器那样显示不安全，我们计划明年明年一月一日才显示为不安全。如果各位 CA 机构，如果你的 CA 系统不支持 CT，原计划是明年一月一日跟谷歌浏览器一样，根信任也没有用，根信任，但是没有 CT 签名数据，零信浏览器一样不信任！现在是 11 月份了，还有很多机构没有完成系统升级，到时候看看要不要推迟，到时再说。

这个是 CT 展示，CT 这块就讲这么多。总结一下，为了保障 SSL 证书的自身安全可信，及时发现错误签发或恶意签发浏览器信任的 SSL 证书，所以有了这个证书透明机制，这个机制很重要，谷歌利用浏览器垄断地位和道德高地实现了全球 SSL 证书监管。同理，国密 SSL 证书，为了保证自己的安全可信，也应该有这个 CT 机制。但是，零信浏览器是个新秀，没有谷歌浏览器那样的垄断地位，我国的国情也不一样，所以，我们通过牵头制定国密标准来实现这个监管，这个标准正在制定中，当然最后一定是密码管理部门来监管，肯定是这样的。希望这种机制像谷歌那样允许 6 家 CT，国家有监管 CT，浏览器也可以提供 CT 服务，也可以要求有一个 CT 必须是国家的 CT，有一个 CT 必须浏览器自己运营的，还会有一个第三方 CT，目前谷歌的要求是至少 3 个 CT 数据，才能保证有 CT 可验证，一个不能保证可用，总有一个能保证，既要透明还要公平公正。就像区块链一样有多个服务节点，保证 CT 系统性能稳定可靠。欢迎大家参与进来，共同保障我国网空安全，因为 HTTPS 加密是互联网的基础安全，而核心就是这个支持证书透明的国密 SSL 证书。

今天我讲两个话题，一个是证书透明，一个是证书自动化，证书透明今天就讲这么多，下

面讲证书自动化，这个更重要。

证书透明是为了保障 SSL 证书的自身安全可信，提供了可靠的生产能力。但是，生产出来干嘛用？当然是为了使用，所以还有一个能力很重要，自动化更重要！只有自动化才能实现快速应用部署。这个我会讲 6 个方面，第一个，什么是证书自动化管理？自动化证书管理，ACME，为什么需要自动化？自动化管理生态是什么样的？产生的效果是什么样的？对我们有什么启发？什么是商密证书自动化管理？为什么我国更需要商密证书自动化管理？还会介绍零信技术打造的证书自动化管理生态，最后，介绍一下我们牵头制定的自动化证书规范国密标准。还会介绍目前国密证书自动化生态情况。

什么叫自动化证书管理环境 ACME？为什么需要自动化管理？因为传统方式申请和部署一张 SSL 证书很辛苦，很痛苦，安装一张证书至少要 1-3 个小时，也许好几天，因为 OV 证书需要等 CA 签发证书，所以，网站管理员需要去服务器上申请 CSR 文件，再找 CA 申请证书，CA 要花两三天签发证书。如果是 DV 证书，马上能发，没问题。但 OV，EV 有可能两三天，五六天没找到人做电话验证，所以，可能一周都有可能。很费劲的把证书拿到以后，再到服务器上去安装，装完以后才实现 HTTPS 加密。它是绕了大圈，用户实际上需要的是 HTTPS 加密，绕了一圈，所以，这很痛苦。怎么办？国际上 Let’s Encrypt 搞了 ACME，ACME 英文就是“顶峰、顶点”的意思，这里是“自动化证书管理环境”的英文缩写，为什么凑这个名字呢？因为这是 SSL 证书的最高境界，到顶了！终极解决方案，顶点解决方案，没有再好的方案了。

自动化，怎么自动化？你只需要在服务器上装一个 ACME 客户端，OK 了，什么都不用做了，自动化给你配 SSL 证书，自动化给你！啥也不用做，永远自动化给你提供 90 天免费证书，到期自动续。再也不需要花钱了，免费全自动，再也不用操心去安装了。这是什么效果？到了什么效果？自动化的效果如何？

咱们看一下这个曲线，看看 Let's Encrypt 的增长曲线，因为是他们发起这个标准，第一个提供这个自动化的服务，火狐浏览器牵头的一个软件厂商提供的解决方案，从 2015 年底开始搞，2016 年开始起步，不到三年时间拿到全球第一的市场份额，现在仍然是全球市球第一的市场地位，遥遥领先。

同志们，我们看看这个最新的统计数据，全球有 6.3 亿张证书，Let's Encrypt 占了 3 个亿，占了一半，其他前七大加起来总和还比他少 400 多万张，为什么？免费，自动化，这是用户所需的。你知道，用户很懒的，我干嘛每年装证书，免费给证书还要装，很麻烦。现在不仅仅是免费给我证书，还自动化，什么都不用管，我只要在我服务器上装一个软件就行了，动一次就行了。这个厉害啊，同志们，自动化！所以，自动化出来以后，他们牵头制定 RFC 标准，RFC8555，标准制定后，谷歌等大厂积极响应。

现在来看一下，第二名是谁，证书量最大的是谁？第二是谷歌了，浏览器厂商，云服务器提供商，第三是 Cloudflare，它是 CDN 起家的，同志们，原先的 CDN 要支持 HTTPS 加密，怎么办？Akamai 全球 CDN 老大,最早提供 CDN 的，不支持 HTTPS，不行的，但必须支持，怎么办？当然后来支持了。像我们国内的云厂商，支持 HTTPS，但需要找 CA 申请证书，再把证书上传上去配置好使用，很麻烦。Cloudflare，只要你用我的 CDN，免费使用，把域名解析过来，OK 了，什么都不用做，我帮你完成域名验证，帮你把证书配好，我帮你启用 CDN，啥都不用管，厉害吧，一下子变成了全球第三大！同志们，这个厉害，这都是自动化的功劳！

第四名是亚马逊，云服务很厉害，它也提供自动化服务，它也做了 CA，做了根，谷歌也自己做了根，做了 CA。所以，他们，谷歌既是 CA，也是云服务提供商。传统的 CA 机构，Sectigo, DigiCert, 变成老五老六了。如果他们不实现自动化，会变老七老八老九，很有意思吧。GoDaddy 第七，微软第八，微软是后起之秀，动作稍慢了一点。所以，这里大家应该是有启发，对不对？

我专门写个一篇 CEO 博客《90 天证书对策四-CA 篇》这个图就是这篇文章里的，引用过来就是要告诉大家，必须走自动化这条路，如果你不走自动化这条路就要掉队！100%掉队，而不管你现在的市场分额是多少，就是这个启发。我们商密 SSL 证书更痛苦，更需要自动化。商密 SSL 证书是什么？怎么更痛苦？我给你一张商密 SSL 证书，没用，因为 Web 服务器不支持商密，浏览器不支持商密，什么都不支持商密，CDN 不支持，都不支持，你给我证书没用，我还要去改造 Web 服务器，改造这个那个，最后才实现了国密 HTTPS 加密，太难了！这个更痛苦。为什么大家都喊国密改造难，更痛苦，因为这是生态改造！难在这里，怎么办？只有一条路，自动化！

刚才讲了国际上的成功经验，自动化经验。那怎么办？国密证书也需要自动化，更需要自动化！为什么说更需要自动化？因为手工搞不定，为什么？因为整个生态都是基于 RSA 密码体系的，自动化只需申请证书，配置到 Web 服务器上去就行了。但是，国密证书不行啊，证书放上去没用，服务器不支持。所以，需要改造，很麻烦。我们更需要自动化。没有自动化，商密 SSL 证书根本不可能普及，不可能！

所以，我们打造了第二个生态，今年打造的。去年我们打造的是国密证书透明生态，今年打造的国密证书自动化生态是把国密证书透明生态产品跟证书自动化生态产品合在一起，合到一个生态去。Web 服务器和浏览器之间要实现 HTTPS 加密，怎么实现？传统安装证书模式不行了，要走自动化模式，我们提供三个解决方案，第一个解决方案就是客户端，跟国外一样的 ACME 客户端软件，客户端干嘛？你可以安装在 Web 服务器中，自动化配双证书，SM2，ECC，自动化配好证书，自动化把国密模块集成到 Nginx Web 服务器中，原 Nginx 卸掉，换成新的

Nginx，支持国密算法的。这个方案用于一个网站还可以凑合用。但是，目前各种操作系统太多了，IIS 改造不了，用不了，只有 Nginx 可以, 但 Linux 有很多个版本，Ubuntu, CentOS，Ubuntu 也有多个版本，都需要适配，所以，这个方案也很难。也没法用，很难真的普及使用，因为要卸载原先的 Nginx，你的业务系统如果正在运行的话，根本不能卸，卸了有影响。所以，这个方案只能说尝试过，我们也有测试网站在用，每天自动签发双证书，在用，但局限性很大。

最好的方法是自动化网关，这是在高交会首发，我们是第一个拿到商密产品认证证书的自动化网关，那么，这个网关能解决问题。自动化，后面会解释。如果客户说我的服务器在云上，我买网关没地方部署，怎么办？所以，我们研发了云服务，把网关部署在云上，给你提供云服务，你买我的云服务，大家共享这个网关，有云服务给你用。所以，这三个方案就可以实现自动化，当然需要云端的支持，云端有 ACME 服务系统，CA 系统，还有证书透明日志系统，这些系统都在云端，我们这是一个端云一体的解决方案，才可以实现双证书自动化，这个叫商密证书自动化。

商密证书自动化管理生态涉及到多个软件系统，如 ACME 客户端，ACME 服务端。如果 CA 机构需要提供自动化的话，你不光是能签发双证书，你还要提供 ACME 接口，基于商密标准接口，对外提供一个接口，参考国际标准提供接口，让客户端、网关可以对接你的服务端，所以，你的 CA 系统是需要改造的，首先是要能签符合标准的商密 SSL 证书和国际 SSL 证书，双证书，另外能够提供 ACME 接口，这些我们都已经搞好了。也就是说，光有“端”是不行的，实现不了自动化。光有“云”也不行，落不了地，落地就靠这个网关来落地。我们这次高交会首发这个方案就是一个自动化解决方案，有证书透明系统，有云 SSL 服务系统，ACME 服务系统在云端，对接网关自动化发证书，你的原服务器在网关后面不用改造，零改造，什么叫零改造？就是不用动，自动给你配好证书，你可以用零信浏览器实现国密加密，其他不支持国密的浏览器用 RSA 加密，没问题。

所以，它是一个端云一体的自动化商密 HTTPS 加密解决方案，这个网关是支持 255 个网站 5 年不间断的自动化配置证书。谷歌把证书有效期缩短到 90 天以后不用怕，自动化的，别说 90 天，一天都可以，每天给你签一张证书，没问题！所以，只有自动化才不用担心证书有效期是一年还是 90 天，还是 180 天，还是 7 天。一年以后变成了半年，变成 90 天，或者 60 天，30 天都很正常，因为密钥越来越不安全了，只有自动化才能搞定这个事，这是我们的一个创新解决方案。这个解决方案，高交会首发，前天在高交会发布会有演示。

目前的使用情况，只有我们在用自动化解决方案。还有很多合作伙伴有兴趣，也看好自动化。

刚才我说了 90 天证书的事，谷歌在推动这事，大家一定要重视，我专门写了四篇文章，

第一篇是政务篇，企业篇、CA 篇、云平台篇，为什么必须重视？因为明年肯定会落地，落地以后怎么办？谷歌为什么推这个？谷歌很有信心，因为已经有 80%的证书已经实现了自动化，现在没有实现自动化的是传统的 CA，阻力在传统 CA，但是在国际组织 CA/B Forum，传统 CA 是没有话语权的，同志们，连续参加过 13 次 CA/B Forum 会议，在会上只有谷歌和火狐在巴拉巴拉一直在讲，CA 是没有话语权，所以谷歌要干 90 天，100%能实现，所以，明年肯定会实现。有人说明年不行，后年也能实现，因为谷歌有绝招，苹果就用过。原来从两年有效期变成一年的时候，CA 当然是反对，但苹果先提出来，不管 CA/B Forum 标准是否通过，没通过没关系，苹果不再信任两年的证书了，那没办法，大家只好乖乖投个票同意了，只好这样了。

所以，我们一定要提前，不能赌这事通不过，一定要相信这个事一定会实现，因为他们有充分的理由，因为目前云计算能力太强大了，量子计算发展也太快了，你的密钥暴露在互联网上一年，反推出私钥出来，国际上密码专家包括谷歌，大家都认为这是有可能，所以，必须缩短到 90 天，只暴露 90 天应该是破解不了的。

所以，这个挑战在哪里？如果是一年期证书，买一张证书，一年装一次还说得过去，如果只有一个网站的话。但是，如果变成 90 天了，一年要装 5 次，不是 4 次，时间要有重叠，有交叉，要提前几天装，所以，工作量翻了 5 倍。我算过，如果一个省政务云有 1 万个网站，实际上不止这么多，像海南省有 18000 个网站，1 万个网站，一个网站安装证书花两个小时，你知道需要多少工程师吗？大概需要 7 个工程师，从年头装到年尾，1 月 1 号开始装，到 12 月 31 号了还没装完，现在变成九十天了，马上要乘以 5，就要 35 个工程师，所以，证书有效期变成 90 天以后，只有自动化这一条路可走，没有第二条路可以走！同志们，要充分认识到这个自动化很重要，很重要！不仅是市场需要，也是你取胜的关键。如果你提供自动化了，就是你取胜的一个重要要素。所以说，只有自动化一条路了，没有第二条路了。

今天讲这个的目的是，总结一下，我们从国际 SSL 自动化管理成功经验里面能看到，国密 SSL 证书的成功之路也是自动化之路，也只有这一条路！同志们，只有这一条路。为什么只有这条路？这条路可以实现零改造，因为只有零改造才能解决国密改造难的大难题。只有自动化才能做到零改造。同志们，这个自动化给了云服务提供商超越 CA 机构，成为主流 SSL 证书提供商的机会，这个非常值得我国的云服务提供商学习借鉴。同理，也值得我国 CA 机构学习。大家都知道，咱们已经失去了国际 SSL 证书的市场份额，但是，通过拿到国密 SSL 证书的市场份额，它配套的国际 SSL 证书市场也就拿回来了！同志们，CA 朋友们，我们大家一起加油，这是大好机会！找回我们市场份额的机会！

这三天高交会期间，我们搞了三次讲座，第一讲 解读密码法，为什么讲这个呢？就是要看准方向，我们干这事，要抬头看路，再埋头苦干，方向错了白忙活，方向对了，事半功倍。

我为什么要讲这个？因为密码法，密码的最大的一个应用就是 HTTPS 加密，因为密码法，密码的最大的一个应用就是 HTTPS 加密，这个也必须讲清楚，不是 USB Key 证书！同志们，密码用于加密保护和安全认证，加密保护在前面，加密保护是最大市场。接着讲了 SSL 证书，数字证书，SSL 证书讲了可靠生产能力和快速部署能力，只有这两个能力都有了，才能去开拓国密 HTTPS 加密市场，普及国密 HTTPS 加密，来保障我国网络空间安全。

感谢大家这次高交会密码讲座的积极参与，今天那讲座就到此结束，谢谢大家！

王高华

2023 年 11 月 19 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。