如何拿下国密 HTTPS 加密大市场？

〈本视频根据 2024 年 3 月 27 日笔者同合作伙伴视频会议技术交流整理，希望更多合作伙伴和潜在合作伙伴能通过观看本视频充分了解零信国密 HTTPS 加密自动化管理解决方案，合作共赢，共同拿下国密 HTTPS 加密大市场。〉

大家好!

现在，各个成熟的业务市场越来越小，并且竞争越来越激烈，怎么办？必须寻找新的蓝海市场。那么，这个蓝海市场在哪里？

大家都知道，现在国际形势严峻，整个互联网的密码体系都是基于 RSA 密码体系的，这个是地基不牢！这块是最核心的东西，所以这个就是国密改造这块的。国密改造这块是一个新的蓝海市场，不管是做密码的，还是做安全的，只有这块才是最大的市场。

为什么说地基不牢？咱们可以看一下两年前俄乌冲突 2 月 24 号发生后，十天之内，第四天就开始禁用和不给俄罗斯发证书了，而第十天开始就完全断供了，这个可能你们不知道。10 天时间，俄罗斯政府的网站、银行网站证书几乎全部被吊销，被断供了，用不了了。所以，现在你去看很多俄罗斯政府网站和银行网站没有证书了。

你想象一下，网银没有 SSL 证书了，你怎么上网银呢？中国政府网如果现在没有证书了，没有 HTTPS 加密了，怎么上政府网站，电子政务服务怎么干？这是个巨大的安全隐患！

所以，国密改造的重点是什么？千万别搞错了。国密改造的重点是国密 HTTPS 加密，这

个最重要。《密码法》第二条定义了密码是用于信息加密和安全认证的，第一是信息加密，那么，最重要的加密在哪里啊？最重要的是 HTTPS 加密，就是传输通道加密。这块改造太重要了，而这个加密只有自动化才能搞得定，后面我会讲。传统模式，你找 CA 买张 SSL 证书搞不定。这个市场是巨大的，是一个百亿级的市场。那么，我们要做好准备，尽快进入这个市场。

那银行这块，给大家看个数据，这是 2023 年 10 月 6 日整理的数据。我国的前二十大银行，看一下这些银行的 SSL 证书的情况，大家看一下这个 SSL 证书的申请情况，工商银行，最大的银行，当然也是申请证书最多的，申请了 672 张，97%都是美国 CA 签发的，如果美国 CA 给断供了，就用不了了，网银访问不了了。它有没有用国密 SSL 证书，有，个别的网站，企业网银，个别网站有国密 SSL 证书。

整个二十大网银中的 85%的 SSL 证书都是国外 CA 签发的，这些证书都有可能被吊销，多危险哦！吊销了，网银就用不了了，风险就在这里。但是，国家要求银行国密改造，本来是要求 2022 年就全部完成的，但是看一下网银系统就知道没有完成！目前只有兴业银行的官网用的是国密 HTTPS 加密，用零信浏览器访问，如果用的是国密，会显示 **m** 标识。你打开零信浏览器访问这个网址，看有没有 **m** 标识，有这个 **m** 就是国密 HTTPS 加密，表示这网站已经国密加密了。

再看一下，工商银行有 672 张证书，你们想象一下，要申请 672 张证书，要给它们装到 672 个或更多个系统里去，多大工作量哦！你知不知道这个工作量，你要养 4 个工程师，至少要 4 个工程师去申请证书，部署证书，安装证书，4 个工程师多少钱，一年费用多少钱？所以，这个是重点，这个是我今天要讲的重点--自动化能大大降低人力成本。这是银行存在的问题，也是很大市场机会。这是刚才说的，机会在哪？机会就是这个必须要替换，必须上国密证书。有些银行没有证书，只要你上网银，看到浏览器显示不安全，那就是没有证书，这就是没有保证银行账户安全。所以说，这个市场有多大，我查了一下，我国共有 4688 家金融机构，你把国密 HTTPS 这个市场做起来，每个银行平均每家要花 200 万，至少花 200 万预算的话，这个市场就 94 个亿！

大家再看一下政府这块，整个全国 31 个省自治区，看看每个省申请了多少张证书，是否启用国密。我这里的统计数据是全国只有一个省--湖南省用了国密证书，全国只有一个省启用国密了，只有一个。整个证书申请量，最少的四川省只申请了 4 张证书。一个省有几万个网站，只申请了 4 张证书，那是因为大量的网站没有证书，大量网站都是明文传输的，很不安全。

为什么你的手机天天收到垃圾短信？因为你上网办事的时候，是明文传输数据的，你数据给窃走了，把你手机号码窃走了，他不需要攻击你的政务系统，政务系统攻击不了，做了很多安全防护，他不攻击系统，但是当数据网上流通之后，他就把数据、手机号码截获走了，因为

是明文传输。你没用 HTTPS，他就非常容易截获你的数据。为什么骚扰电话那么多，就是这样被泄的。你做了用户数据保护了吗？你根本没有保护好用户数据！

那么，这个 SSL 证书数量跟港澳台数据对比一下，整个大陆的所有政府网站只有 16917 张，而台湾一个省就有 12534 张，香港有 2023 张，2023 张比 31 个省的总和还要多。香港只是一个城市，31 个省加起来才 1555 张，还差 24%，只有三分之二！你说这个普及程度差多远，差好远。更没法比美国了，美国是 100% 200%的有证书。所以，这个市场也是非常大，非常大！

市场机会巨大，有多大？我大概估算一下，每个省的政府平台，如果把它全部实行国密加密的话，31 个省，每个省 3000 万，就是 9 个亿。28 个部委，每个部委 2000 万预算，就是 5.6 亿。36 个省/副省/厅级市，每个 1000 万，就是 3.6 亿。央企，也必须国密改造，每个企业 500 万，就是 4.9 亿。加起来的市场总规模就是 23 个亿，够不够！

所以，我在想这么大市场为什么等着我们，为什么没动静？为什么没人去做？为什么大家不做？我可以告诉你答案，为什么没做？为什么这么多系统不做？有难度啊！同志们。我跟银行交流过了，跟政府部门交流过，有难度啊！他们说：我搞不定，我没办法。

难度在哪里？难度重重啊！何止一点难啊！浏览器、移动 APP 不支持国密，Web 服务器不支持国密，加密增加负担。目前市场上 CDN/WAF 不支持国密，传统 CA 系统不支持，不能签发国密 SSL 证书。改造工程复杂，无从下手，怎么办？改造有风险，对业务入侵很大！我的业务系统不能动，你让我改造，我也改造不了。不能动，我要保证我的业务正常运行，保证能提供服务！用户不关心，用户可能不懂，不知道有没有 HTTPS 加密。但是，用户要知道系统用不了了，不行。问题就在这里，我的业务系统不能动，我要保证业务系统正常！加不加密，领导不懂，不知道。用户也不懂。是不是泄露了数据，让别人拿走了，反正没发生事故，我也不知道。

就是这 6 个问题。这些问题，纠结在哪里呢？纠结在整个密码体系，是 RSA 密码体系。很难改造一个生态，整个所有生态产品，从底层到中层到应用，各个方面都是 RSA 密码体系。打了形象的比喻，这个 RSA 体系已经四十多年了，深圳是四十多年的城市，你想把城市的自来水水管全部换掉，可能吗？太难了换不掉，对不对？难！所以，为什么只有一个银行用了国密，一个省用了国密，并且只是官网用了国密。说实话，国密改造太难了！

这还不是最难的，同志们，最难的哪里啊？最难的，今年会出现。为了保证 SSL 证书的密钥安全，谷歌去年 3 月份就开始推动 SSL 证书有效期变成 90 天，你们知不知道，现在的 SSL 证书是一年有效期，国际标准只允许发一年期证书，从 5 年，以前允许发 5 年，改为发 3 年，发 2 年、发 1 年。因为，现在云计算、量子计算，算力太猛了，密钥不安全了。谷歌率先推动证书密钥 90 天必须换一次，因为公网 SSL 证书，在互联网访问的时候，公钥是公开的，如果

时间太长了，会反推出私钥。所以，要改为 90 天，今年会落地这个政策。

去年 3 月份谷歌在推动，如果这个国际标准 90 天落地了，我估计今年会落地，落地是什么概念呢？

你以前网银用了 600 多证书，工行的，每年去申请一次，申请 600 多张，去安装。现在，如果变成了 90 天，每年要申请 5 次，等于要安装 3000 多证书。那以前要养 4 个工程师，我现在要养 20 个工程师来要干件事，那就更难了，那根本干不动了！那就是真的是干不动了，干不动了！如果变成了 90 天，绝对不可能手动装证书了。就像每个省政府，一个省政府有 16000 个网站，我算个，16000 个网站，你要养 20 多个工程师，

从 1 月 1 号开始装证书，一直装到 12 月 31 号，还没装完！那养 20 个工程师要多少钱？所以，这个事没法干！手动不行，必须自动化！

我总结了 7 大难点，这事根本干不了！所以还没有人干这事！那就是说没戏了？戏当然有啊！没戏，我下面就不用讲了，对不对？当然有戏！

所以，我反复宣传，国家为什么要求你上国密，是为了你的业务系统安全，因为你的证书被吊销以后，

你的网站就访问不了了，用户上不了网银怎么办？你不要只是为了应付检查，而是应该为了保证业务可靠的运行！这个才是最重要的。我打个比方：为什么开车不能喝酒？不是交警不让这样干，实际上是为了你的安全！你喝酒撞死人了怎么办？你老婆还在家里等着你啊！你要是认识到这个高度就对了，没有这个高度你就是应付检查，你肯定迟早会出事！这就是我们在做销售的时候，我们要跟客户讲这个，要同客户讲清楚这个道理。

OK，我们回到主题。7 大难题，同志们，我们必须提供解决方案给用户。我们有解决方案，零改造、零安装、零维护，全自动实现国密，解决太难的问题。你原先难，现在什么都不用做，什么都不用改造，

不用安装，不用维护，全自动，那难就变成了不难，这事你就可以干了，不难了！这就解决了难的问题。

那么，我要解决这么难的问题，就需要一套很复杂的系统来实现自动化，那这个单就很大了，所以把单小的问题也解决了。太难和单小的问题，我一个方案就解决了，两个问题都给你解决了，独家打造！十年磨一剑！当然，我这个方案只用了 3 年时间打造！

所以，这个方案，到底什么方案？一定是个自动化的方案！自动化搞定的国密改造方案。我们平常给用户的产品给对了吗？到底用户需要什么产品？现在，所有 CA 都是卖证书，那么，用户买证书，申请证书，再到服务器上安装，装完以后再实现 HTTPS 加密，很麻烦。但是，用户实际需要的是实现 HTTPS 加密，保证传输通道安全，保证数据安全。所以，用户不是需

要 SSL 证书！所以，我们要反思一下，我们是不是给对产品了？我们不应该卖 SSL 证书，不是用户要的东西，用户需要 HTTPS 加密。

如何实现这个目标？国际上解决方法叫 ACME，ACME 什么意思啊？就是自动化证书管理环境的缩写。实际上，这是套用了个单词 acme, 顶峰、终极的意思，就是终极解决方案，自动化。自动化怎么做？怎么自动化？你什么都不用做，我给你一个软件，给你一个 ACME 客户端软件，你装到服务器上实现自动化，给你申请和装好证书，自动化的，你什么都不用做，一次性装软件，就行了。这是国际上解决方案，叫 ACME。谷歌想推动 90 天证书是有底气的，国际上已经做到了，百分之八十以上 SSL 证书中都已经自动化了，做到了自动化，那就不需要手动装证书了，国际上已经做到了。

OK，那么国密这块？我们也需要自动化！我们做国密也只有自动化这条路，国密自动化比较难一点，国密自动化需要国际的自动化，再加上国密证书，加上国密模块。所以，国密自动化这块，装个软件没用，

跟国际上的方法不一样！我们打造的一个方案，就是一个双证书的方案，就是有一个网关，我们叫零改造，

你的网站，不需要装证书，什么都不用做，前面加个网关就行了。

现在市场上有网关产品，并不是没有网关产品，你可以搜下，很多公司做网关，传统的 SSL VPN 网关，综合网关都有，它怎么做的？需要你去找 CA 申请 SSL 证书，它也支持国密，要求你把证书装进去。还是逃避不了传统的 Web 服务器一样装证书原理，你要找 CA 申请证书，要去配置，如果是 90 天证书，每年申请 5 次，安装 5 次。

我们怎么解决啊？我们是端云一体，端就是网关。对，端云一体，网关自动到云上去自动化给你配证书。用户不需要装证书，网关是含证书的，管 5 年证书，管 255 个网站，双证书自动化给你配，你什么都不用做！云端自动化给你配证书，这个证书有效期到了之后，通过网关自动去申请新的证书。你什么都不用做，你只要把网址配好，它自动给配证书，证书到期，自动签发给你。给你自动化装好，保证你网站是 5 年 365 天国密加密的。

你的网站原来是在互联网可以访问的，你本来有公网 IP，你只需要把公网 IP 移到零信网关上，就行了，把域名解析到网关上就可以了。由网关来自动化申请证书，由网关来自动化提供 HTTPS 加密，不是你的服务器，服务器 HTTPS 加密的工作量全部移到网关上，申请证书的工作量也是网关的，你的服务器专门用于业务系统了。

不仅原服务器不用动，也不用装证书，而且我们还免费配套一个国密浏览器给你--零信浏览器，因为你需要浏览器来实现国密 HTTPS 加密。零信浏览器是免费的，不是像外面市场卖的贵，收费的。零信浏览器是完全免费的，配套的国密浏览器。零信浏览器，现在是中国市场

份额第一的国密浏览器，因为其他国密浏览器都是收费的，而零信浏览器是免费的，所以大家都喜欢用零信浏览器。零信浏览器更好，零广告，干净，免费，国密浏览器没广告！

所以，这是端云一体的一个解决方案。大家可以看一下，云上有证书透明系统，云 SSL 系统，证书自动化服务系统，签发系统自动化给你双证书，给你国际信任的 ECC 证书和国密证书，双证书。为什么需要双证书？因为你不能限制网银用户用什么浏览器，用户要用谷歌浏览器怎么办？你也得让他用。所以，你如果用谷歌浏览器，就用 RSA 加密、ECC 加密。如果你用零信浏览器，就用国密加密。两种算法的证书都必须得有，都在网关自动配置好双证书，都是双证书。现在国密改造，都是双证书，没有单证书的，因为你不可能限制用户使用何种浏览器的。

这是一个端云一体的方案，这个方案我们是全球首创，在去年 11 月份高交会首发，首创首发，并且高交会组委会给我们颁发了一个优秀产品奖。这个网关产品，我们用了 5 个月时间拿到商密产品认证证书，这是我国第一个叫国密 HTTPS 加密自动化网关的产品。以前的网关都是什么安全网关、SSL VPN 网关,
什么什么网关等，我们是只做 HTTPS 加密的自动化网关。

我们的产品自动化做好以后，就牵头制定这个《自动化证书管理规范》标准。为什么要制定这个国密标准？为什么？因为这块太重要了，没有标准不行！再加上《证书透明规范》，这两个标准都是参考国际标准 RFC8555 和 RFC 6962 两个国际标准，我们把它变成了国密标准。所以，我们的产品，我们的生态，不光是有产品，不光是实现了，还牵头制定了国密标准，大家都一起按照标准这样做。这是我们做的一个 HTTPS 加密自动化标准，也可以证明我们的产品研发实力。

OK，我就介绍一下零信网关，这是重点。传统模式，你要买一张国际 SSL 证书，装到服务器上去，很麻烦。但是，这只是 RSA 加密的。那么。现在中间加个网关，什么都不用做，连接云端，它自动给你配置国密证书，就可以实现国密 HTTPS 加密了。所以，它是一个零改造的、自动化的、解决方案。

这是网关产品，一个独家解决方案。有的客户说，说我的机房没法部署网关，或者说我的网站很少，因为零信网关支持 255 个网站。没地方部署网关怎么办？我们有网关部署在云上，你可以共享，买我们的云服务。我们把网关部署到云上，可以给大家共享这个服务，给你云服务，你只需要做个 CNAME 解析就可以了，一样可以做到 HTTPS 加密零改造，什么也不用做，一分钟就搞定。

我们有个合作伙伴，他就是提供云服务。政府没钱，买不了网关。他来买网关，他把网关直接部署到政务云，政府想开通某个网站 HTTPS 加密就找他开通，设置网站域名就开通了，

按卖证书钱来收钱。他算过账，投资 1000 万元，可以收回 5000 万元。因为我这个网关是管 255 个网站，证书管 5 年，后面会讲这些证书值多少钱。结果他一算帐，赚老了。所以，这是一个不同的运营思路。

到底是卖网关挣钱，还是做卖服务挣钱，都可以。你要卖服务挣钱，你就把网关架上去。你投网关进去了，当然你必须搞定关系，不然客户如果不用你的，那就白投资网关了。所以，这是不同的商业模式。

OK，我们这个体系，之所以能完成这个自动化，就需要一个端云一体的解决方案。有浏览器，因为要两端，用户端和网关端。浏览器，目前市场上的国密浏览器都是收费的，没法完成国密改造，不可能所有用户都花钱去买浏览器。全世界没有这种先例，哪个国际大厂浏览器是收费的？没有，这是乱搞的，这是其他国密浏览器厂商的短视行为！所以，我一定要做一个免费国密浏览器，因为你要普及国密。全世界 RSA 密码是怎么普及的？是因为有四大浏览器哦。谷歌、微软、火狐、苹果，他们都是免费的，大家都可以用，可以免费使用。所以，我们要做免费的国密浏览器。所以，我们零信浏览器，免费国密浏览器，我们免费国密浏览器，已经在中国市场份额第一了！

HTTPS 加密是两端，浏览器和服务端，所以，我们要做两个端--浏览器和网关。那么，云端有证书透明日志系统，有云 SSL 系统，有自动化证书管理系统，它必须端云一体，自动化实现 HTTPS 加密。我说一下这个自动化，怎么实现自动化的。网关第一个角色，是充当通讯协议的转换，从 HTTP 协议转换为 HTTPS 协议，原来是 HTTP 的，通过网关就变成 HTTPS 了，什么都不用做！那第二个作用，就是起到两个密码体系转换的作用，原来你是 RSA 的，我用国密实现，RSA 密码体系变成国密体系。你原来如果有 RSA 证书，那么当然 RSA 回源给你。网关在这里做了两个协议的转换，两个密码体系的转换。

那么，这两个转换依赖于自动化，怎么自动化？有云 SSL 系统，没有这个自动化，没有这个云 SSL 系统，实现不了。这是我们这个端云一体的价值。它价值体现在哪？这个自动化管 255 个网站，这个自动化可以让你省两个工程师的费用，两个工程师没有事干，不用两个工程师了。这两个工程师 5 年，一个月工资 12500 元，两个工程师乘以 12 乘以 5 年，就节省你的人力成本 150 万！这是第一个价值，自动化带来的价值，节省工程师的人力费用。

第二个价值，双证书的价值。双证书，国密 SSL 证书和国际 SSL 证书，双证书，给你节省的价值是 623 万元。怎么算出来的：5 年 255 张，你在我们官网去买证书的话，OV 精简版，国密 OV 加国际 DV，这样的双证书一年要 4888 元，你自己买证书的费用。这个 OV 是什么意思？OV 就是 Organization Validated。

SSL 证书有 DV/OV/EV 三种，OV 就是证书里面显示单位名称。DV 呢？只显示域名，不显示

单位名称，不验证单位名称。EV 呢？扩展验证单位身份，地址栏变绿色的是 EV。

各种证书费用是不一样的，如果你要低端双 DV 的话，价格是 988 元，5 年证书也值 230 万元。但是，我们现在配的是国密 OV 加国际 DV，国密用 OV，让你显示单位名称。国际用 DV，不用提供身份证明材料。因为你要显示单位名称，必须提交身份证明材料，可是政府单位提交不了，所以就不用提供了，给 DV 证书。

看看零信网关，你们觉得网关能卖多少钱？你看看，已经给你省了 150 万的工程师人力成本，已经给你里面含了价值 623 万的双 SSL 证书，所以，为什么刚才说那个合作伙伴，他不卖网关卖服务，每增加一个网站，收 4888 元，255 个网站 5 年就是 623 万。一台网关的投资能够收回 623 万证书的钱，就这个概念。为一个网站启用一张证书，收用户 4888 元。你们到网上搜一下证书价格，现在卖的更贵的都有，有卖 6888，卖 9888，卖 13000 的，多的是，你们在网查一下。我们这个 4888，是我们卖的双证书价格，你在网上买证书的价格，你去买证书的话，就是这个价格。第二个价值，就是证书超值！

第三个超值，你的网站为了安全，一般都会采购 WAF 设备。WAF 设备，就是 Web 应用防火墙，它防护网站的攻击，它是 HTTP 流量过来以后拦截攻击流量，就是前面加了 WAF 设备。这是一个买 WAF 设备的方案。第二个呢？可以是云服务，如阿里云、腾讯云、天翼云，都提供云 WAF 服务，每个网站几千块钱，几万块钱。两个方案都可以实现 WAF 防护。

而网站为了实现 HTTPS 加密，当然需要装 SSL 证书，怎么装？还是一样，还是要用户找 CA 申请证书，配置到 WAF 设备中，配置到云服务中去，上传 SSL 证书，跟传统 Web 服务器安装证书是一样的。只不过你不用装到 Web 服务器上，装到 WAF 设备/云服务上而已。所以，还是人工的方式。

那么，我们解决了什么问题？零信网关内置 WAF 模块，自动化给你配证书，什么都不用做!而这个 WAF 模块的性能怎么样？大家可以上一个国际上有名的 WAF 测试网站--WAFER，专门测第三方 WAF 性能怎么样的。我们测了一个网站，测零信网关 WAF 防护的网站，能够达到 B 级，检测能力达到 B 级，识别能力达到 A 级，很厉害了，这个水平，相当于售价 100 万元的 WAF 设备的水平！市场上卖 100 万元的 WAF 设备也就是水平，甚至比我们的还差。那么，它能拦截什么？能拦截这么多。100% 拦截服务器端包含注入，跨站攻击 98%拦截，SQL 注入 98%拦截，85%拦截目录遍历攻击。你们都可以拿到网关后去测，这不是我说的，不是我吹的。

也就是说，零信网关里这个 WAF 模块，内置的，免费配套的。所以，免费内置 WAF 模块，是第三个价值。网关内置 WAF 模块提供 HTTPS 加密加 WAF 防护，这个 WAF 功能值 100 万元！你看零信网关的价值多厉害，加上证书值 623 万、节省 150 万人力成本，这就是全部价

值，你 100 万卖给用户，用户一点都不嫌贵。所以，零信网关有三个超值。

零信浏览器，这是乌镇首发的一个产品，2022 世界互联网大会首发，不仅支持国密加密，并且还支持 PDF 验签，这是全球唯一的一个。你打开 PDF 文件，无缝打开 PDF，其他浏览器也能打开 PDF，但是，里面有数字签名，它不知道，不显示，你用谷歌浏览器打开试下。

用零信浏览器访问零信官网，看我的 CEO 博客，我的 CEO 博客每一篇文都有数字签名，打开 PDF 文件里面有数字签名，零信浏览器可以验我的数字签名，这是集成的 PDF 阅读器，下一步我们要集成邮件客户端，邮件加密。

所以，零信浏览器，我们的目标是三年之内全球老二，现在已经是中国市场第一的国密浏览器，因为功能太好了，太好用了，并且是免费的。

我这里再举一个银行的部署方案，银行有中心机房，有本地服务器给本地转发，外地分行支行可以通过 HTTPS 方式统一集中提供 HTTPS 加服务。我前面讲了，可以提供云服务，也就是说，这个网关不光是为你本地机房的网站提供 HTTPS 加密服务，还可以为外地网站提供服务，只要能够通过内网或者通过外网，通过互联网能够回源，能够连过来就可以了。它是个集成的方案，你买一套(两台、四台)，那么，分行、分支机构、办事处，都可以实现 HTTPS 加密，都可以为你的业务系统实现 HTTPS 加密自动化。

最后，你们看看广西自治区人民政府的网站，你们自己访问一下，没有证书的，显示“不安全”！很多省政府网站都没有证书！你看看部署网关以后，你看看效果，看这个标识，有网关。部署网关后就国密加密了！同一个网站，你只要部署了网关或者云服务，你做 CNAME，把这个域名做 CNAME 就可以了。CNAME 解析到网关，就变成国密加密了，就一分钟的事情！启用国密加密，搞定，就一分钟的事！

我们再看中国政府网，有 RSA 证书，是 RSA 加密的，也有 WAF，没问题，但是没有国密，而经过网关回源后，就有国密了！国密 HTTPS 加密。我们在电信机房部署的零信网关里面有很多实验网站，有 HTTPS 交付设置，交付就是设置网站，把网站添加进去设置就可以启用国密 HTTPS 了！

那今天先讲这么多，谢谢大家！

王高华

2024 年 5 月 10 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 164 篇(共 44 万 5 千多字)和英文 65 篇(7 万 9 千多单词)。