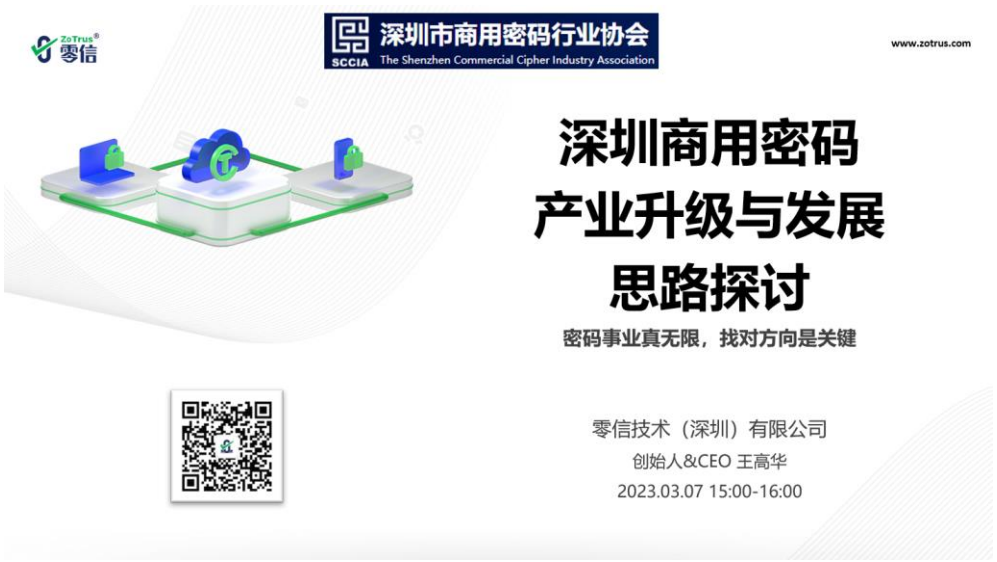
深商密协会讲座 | 深圳商用密码产业升级与发展思路探讨

深圳市商用密码行业协会于 2023 年 3 月 7 日邀请零信技术创始人&CEO 王高华给协会全体会员做了商密产业升级与发展思路探讨的讲座，本文根据讲座内容整理。

本次讲座王高华从 4 个方面给出了对深圳乃至全国的密码产业发展的思考和思路，首先解读了我国的《密码法》和美国的《联邦零信任战略》，接着解释说明商用密码事业发展的大商机已经来临。而如何抓住这个大商机，王高华就自己重新创业的亲身体会举了 3 个例子说明如何准确定位产品，提供用户真正所需要的产品。接着谈了 7 个方面的密码应用畅想，展示一下密码应用的大好前景，希望同深圳商密产业界朋友一起不忘初心齐努力，共同打造深圳密码产业新高地。



一、解读《密码法》和《联邦零信任战略》

王高华认为：密码产业要发展，当然首先要学习《密码法》，学法懂法才能找到我国密码事业发展的大方向。而最重要的是《密码法》第二条对密码的定义：**本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务**。接着从 4 个维度讲清楚密码的形态、用途、技术路线和保护对象，第二条对密码的定义给我国的密码从业者指明了方向。

第一：明确定义了密码的形态

密码是一项技术，称为密码技术；也可以是一种产品，称为密码产品；也可以是一种服务，称为密码服务。密码以三种形态存在，可以是技术、产品和服务，这为密码从业者指明了发展方向，可以从事密码技术研究，可以从事密码产品研发、生产和销售，也可以提供密码服务，以服务形式来提供密码产品，通常指云密码服务或称密码云服务。

第二：明确定义了密码的用途

密码用于加密保护和安全认证，准确理解这个用途非常重要，给密码从业者指明了密码到底该用在什么地方。第一个用途是加密保护，这是用途最广泛的应用，如 HTTPS 加密、数据加密、邮件加密和数字签名、文档加密和数字签名、软件代码数字签名等。第二个用途是安全认证，用数字签名技术来实现安全可靠的用户身份认证。

第三：明确定义了密码的技术路线

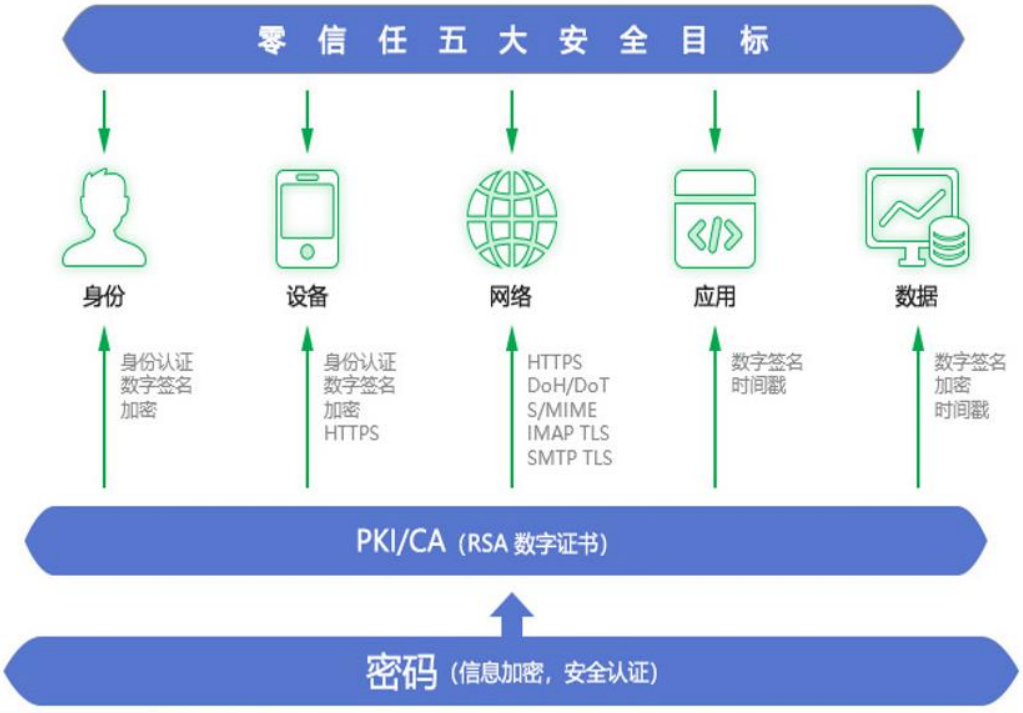
通过特定变换的方法来实现，这个特定变换的方法就是密码算法，用密码算法来实现特定变换。特指商用密码算法，如：SM2、SM3、SM4 和 SM9 等，不包括国外的密码算法，这一点非常重要，一定不能搞错。

第四：明确定义了密码的保护对象

是信息等。信息需要用密码来实现加密保护，信息同时需要密码来实现安全认证后才能获取。等就是所有其他元素都可以用密码来实现加密保护和安全认证。

接着又解读了美国《联邦零信任战略》，解读这个战略是希望能找到密码落地应用的思路，如何用密码来保障我国互联网的安全和保障万物互联的安全。美国联邦零信任战略从身份可信、设备可信、网络安全、应用安全、数据安全等五个方面来规划美国联邦政府机构安全地从传统的安全架构转向零信任安全架构。这个战略的核心实际上是密码的全面应用，用密码技术来保障网络流量的安全，包括 DNS 加密、https 加密和邮件加密。王高华还补充了如何用密码来保障零信任模型的五大支柱的安全，包括身份可信、设备可信、网络安全、应用安全和数据安全，都是用数字证书来实现数字签名和加密，并强调千万不要以为零信任就只是身份认证这一个应用，是五大应用！这也是我国的零信任安全市场的最大误区和差距。

而对于 https 加密，这是密码在保障互联网安全的基础应用。联邦零信任战略要求所有政府.gov 网站必须强制实现 https 加密，无论是外网还是内网，这是对 http 明文传输的零信任！不仅要求 https 加密，而且已经同各大浏览器合作预置设置浏览器只能用 https 来访问.gov 网站。这些都值得我们学习。



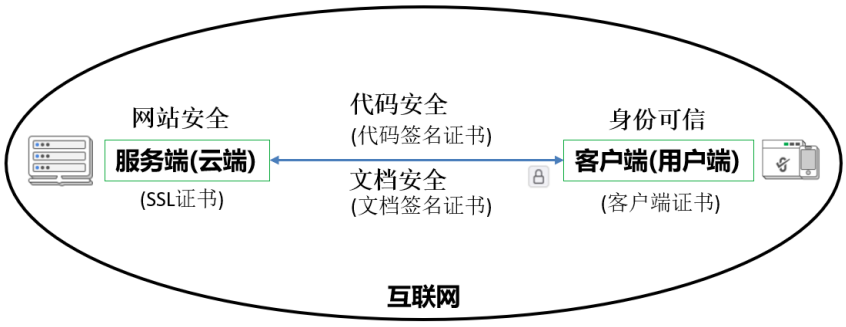
王高华认为：我国的《密码法》就是中国的零信任战略，一个比美国的零信任战略更有高度的战略，不仅仅是“永不信任和始终验证”，而是“永不信任、始终验签、始终加密”，对没有采用密码保护的信息和身份零信任，这个零信任的理念在《密码法》第二十七条就已经有明确要求和第三十七条的处罚有明确的规定。

美国联邦零信任战略对密码产业界的启示是，我们应该对零信任模型的五大支柱提出基于密码的解决方案，包括身份可信、设备可信、网络安全、应用安全、数据安全，而不只是一个解决方案—用户接入认证，其核心是密码的全面应用，这里商机无限。

二、密码事业发展大商机已到

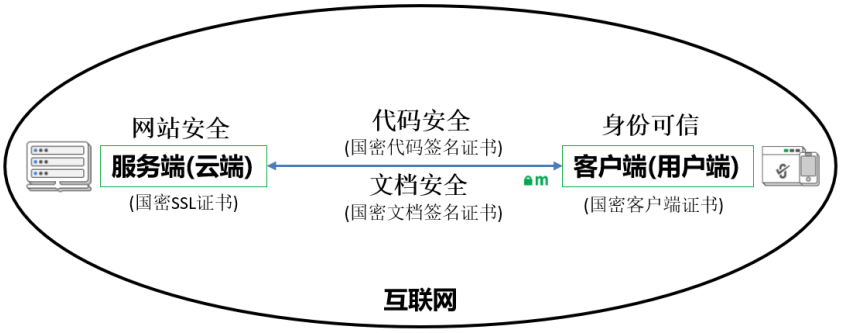
王高华首先解释了复杂的全球互联网其实并不复杂，可以简化为只有两端：服务端(云端)和客户端(用户端)，服务器的安全采用 SSL 证书实现 https 加密来保证从用户端浏览器到服务器之间的通信是加密的，客户端的安全可信采用客户端证书来实现安全认证，也可以用于邮件加密。而中间跑的代码安全由代码签名证书来实现软件代码数字签名和时间戳，文档安全则由文档签名证书来实现文档数字签名和加密。由这 4 种数字证书来保障全球互联网的数据通信安全和身份可信。

基于RSA密码体系的公钥基础设施(PKI)，用于保障全球互联网(万物互联)安全



但是，俄乌冲突发生后的俄罗斯政府网站和银行网站的 SSL 证书被恶意吊销和断供，这给我国互联网的安全敲响了警钟。为了保障我国互联网安全，我国必须采用国密 SSL 证书来实现 https 加密，以免将来可能出现俄罗斯一样严重的互联网安全事件发生，必须全面采用商用密码来保障我国互联网的安全，这是商用密码产业发展的大好机会，我国的商密企业包括深圳商密企业应该抓住这个机遇，加大研发投入和市场拓展力度，来推动采用各种商用密码数字证书来保障我国互联网安全和万物互联安全。

基于商用密码体系的公钥基础设施(PKI)，用于保障我国互联网(万物互联)安全



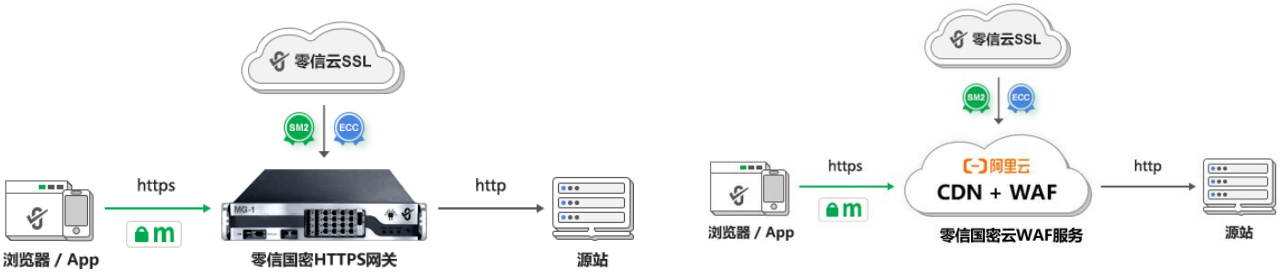
而如何落地密码产品和密码服务，则可以借鉴美国联邦零信任战略，全面采用密码产品或密码服务实现数字签名和加密来保障设备可信、身份可信、网络安全、应用安全和数据安全。每一个细分的密码应用市场都是一个很大的市场，这是一个巨大的市场机会，深圳商密企业乃至全国的商密企业都应该抓住这个机会，提供各种相应的产品和解决方案来保障我国互联网安全。密码的最大市场在网络安全产业，用密码产品和服务来保障网络安全。

三、举例说明，以期启发

如何抓住巨大的商用密码应用市场机会，王高华举了 3 个例子说明如何准确定位产品，如何换一个思路实现国密改造，如何打造一个大家一起合作的生态。

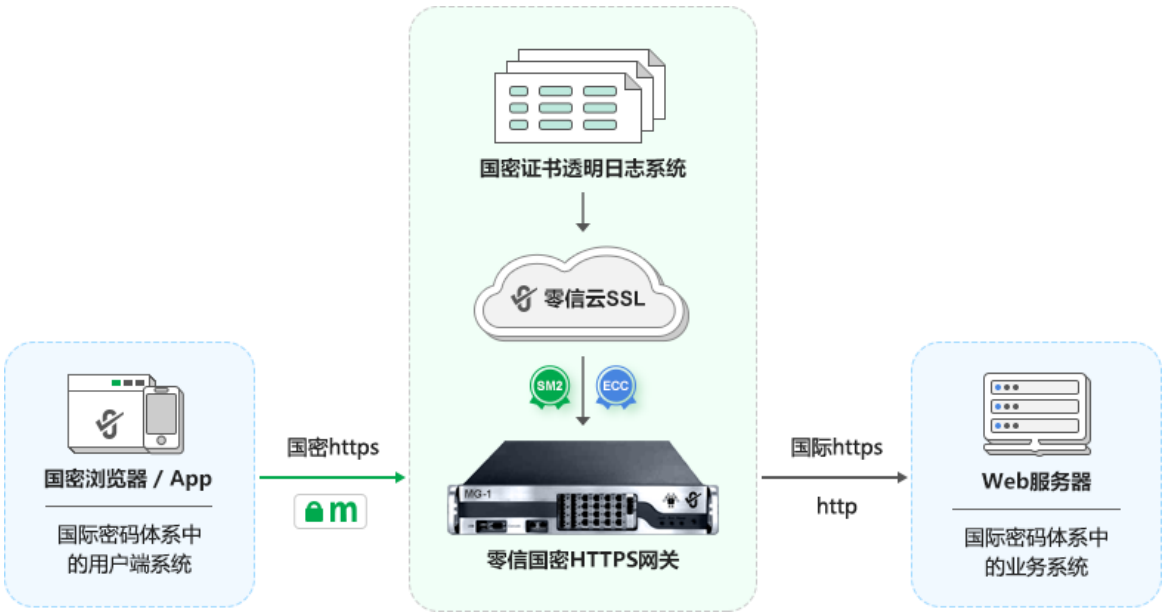
第一个例子是如何准确定位产品，需要问自己两个重要的问题：用户到底需要什么产品？我们给对产品了？王高华以自己熟悉的 SSL 证书为例，说明思考了这两个问题后才找到了准确的用户需求：SSL 证书真的是用户需要的产品？不是，用户需要的是 https 加密，需要的是消除浏览器的“不安全”警告，需要的是国密合规！而不是 SSL 证书！我们应该研发和销售 https 加密产品，而不是 SSL 证书！这个重要的思考和发现值得所有 CA 机构反思。

正是由于有了这个思考，所以，零信技术不再是为用户提供 SSL 证书，而是为用户提供能自动化配置双 SSL 证书的硬件密码产品—国密 HTTPS 网关，为用户提供能自动化配置双 SSL 证书的密码服务—国密云 WAF 服务，由网关和云服务来完成双算法双 SSL 证书的申请、部署和续期等繁琐的 SSL 证书全生命周期管理，由网关和云服务来直接为用户提供 https 加密服务，并且是双算法自适应 https 加密。



第二个例子是关于国密改造，很难！因为目前的互联网安全体系是基于 RSA 密码体系打造的，用户常用的浏览器和 APP 不支持国密算法、常用的 Web 服务器不支持国密算法、传统 CA 系统不支持签发国密 SSL 证书，常用的 CDN/云 WAF 服务和 WAF 设备不支持国密算法，现有业务系统复杂，要实现国密改造很难，这就不难理解为何目前最常见的国密改造项目居然是门禁系统了，因为容易改造哦。而对于正在运行的业务系统，改造风险极高，不好改，最关键的一点是不能影响现有政务系统的正常可靠运行，各个局委办的网站都在政务云平台统一管理，有成千上万个政务网站在正常运行，动任何一台物理服务器就可能把某个关键系统给影响了，那就是大事故！绝对不能出事，这一点是第一重要的事情，而把现在的 http 网站升级为 https 加密和国密 https 加密变成了次要的事情。但国密改造必须做，这就很纠结，很矛盾。

零信技术给出的解决方案是零改造，现有系统很难改造那就干脆不改造，在现有系统前面增加一台国密 HTTPS 网关，并且由网关对接零信云 SSL 系统实现自动化配置双算法双 SSL 证书，当然是配置的双 SSL 证书都支持证书透明，以保证 SSL 证书的自身安全可信。而用户端只需让用户改用支持国密算法的浏览器即可，如完全免费的零信浏览器。至于常用的 APP，都是大厂出品，增加支持国密算法应该不难。这个新的思路值得大家借鉴，就是国密改造难，干脆就不改造，零改造完成国密改造！



第三个例子是打造生态，大家一起玩。基于公钥基础设施的互联网安全体系要全部支持国密算法，这是一个大工程，需要建立一个生态，让各个相关厂商都参与到这个生态中来，只有这样才能让这个生态真正实现良性循环。零信技术打造的第一个生态是国密证书透明生态(SM2 CT)，这是一个借鉴国际证书透明生态打造的支持国密算法的生态系统，包括采用国密算法实现的证书透明日志系统、能签发支持国密证书透明的国密 SSL 证书的国密 CA 系统、能实时验证国密 SSL 证书中的国密证书透明日志签名数据的国密浏览器，还有基于国密证书透明日志系统的第三方国密 SSL 证书签发数据分析、监督和审计服务，这 4 方参与者共同打造国密证书透明生态，共同保障国密 SSL 证书的可靠供给和可靠生产能力。

零信技术历时一年多时间开发了这 4 个方面的 4 个产品：零信国密证书透明日志系统、零信云 SSL 系统、零信浏览器和零信证书透明数据查询系统，自己形成了一个完整的生态，这就给相关厂商证明了各个生态中的产品的可行性，让大家可以体验生态是如何运作的。并

且，零信技术还正在牵头制定证书透明国密标准，让这个生态的参与者可以按照统一的标准参与到这个生态中来，共同提供可靠的国密 SSL 证书生产能力。

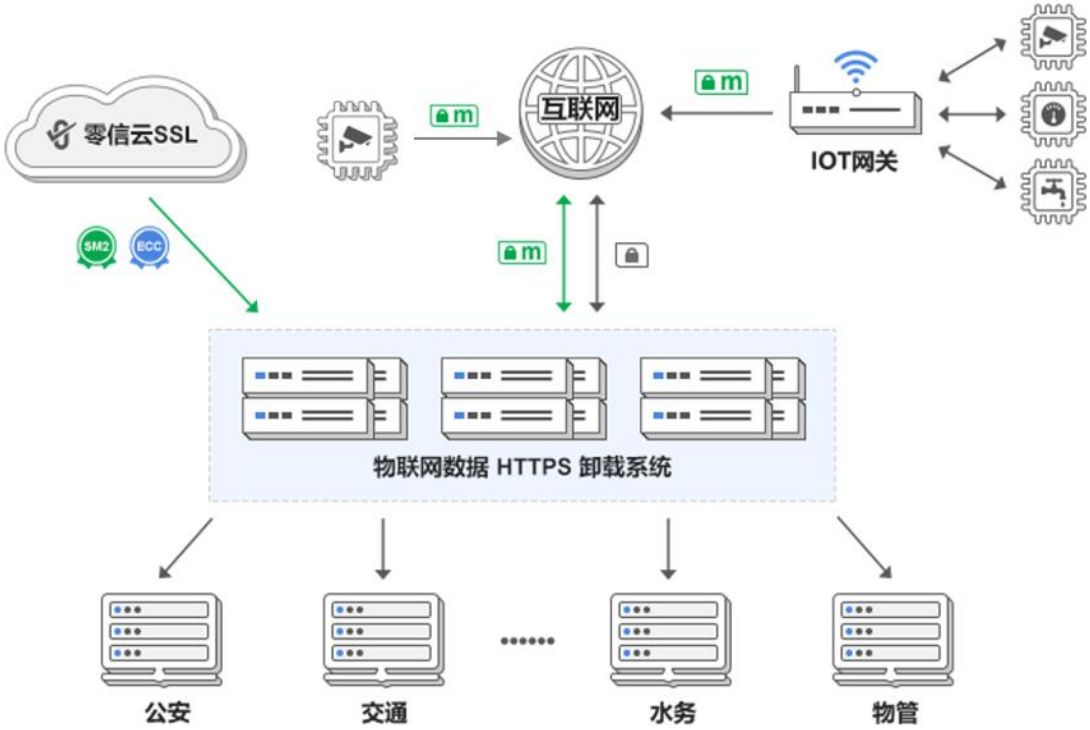
而要普及国密 SSL 证书的应用，光有生产能力是不够的，必须有国密 SSL 证书的快速部署能力。所以，零信技术又打造了第二个生态—国密证书自动化管理生态(SM2 ACME)，这个生态专为国密 SSL 证书的快速普及应用打造。这个生态包含了国密证书透明生态中的多个产品，包括增加了国密 ACME 服务系统的零信云 SSL 系统、双算法双 SSL 证书、国密证书透明日志系统、零信浏览器，同时创新研发了国密 ACME 客户端、国密 HTTPS 网关和国密云 WAF 服务。并且，零信技术还正在牵头制定证书自动化管理国密标准，让这个生态的参与者可以按照统一的标准来参与到这个生态中来，共同打造国密 SSL 证书的快速部署能力，为普及国密 SSL 证书应用提供各种可行的解决方案。

四、国密应用畅想

王高华在讲座的最后一部分谈了 7 个方面的密码应用畅想，展示了密码应用的大好前景，希望同深圳商密产业界朋友一起不忘初心齐努力，共同打造深圳密码产业新高地。

这 7 个应用畅想包括密码在物联网的应用、密码在物联网设备安全的应用、密码在车联网的应用、密码在智慧城市的应用、密码在工业互联网的应用、密码在文档安全的应用和密码在电子邮件安全的应用，这些应用都是用密码产品实现 https 加密、文档数字签名和加密、电子邮件加密和数字签名、身份认证、数据加密、时间戳等等。特别指出了目前的物联网的各种设备包括各种摄像头都是明文传输数据到云端，这非常不安全，非常容易遭遇数据篡改

和攻击，必须采用 https 加密方式实现物联网设备、车联网设备、工业互联网设备的数据采集与传输，只有这样采用保障智慧城市系统的数据安全和可靠运行。



五、总结

在讲座的总结阶段，王高华给大家推荐了两本书，一本是《巨人的工具》。他认为马克•安德森说得很有道理：最优秀的商业模式是你提供好产品、消费者付费，然后你赚钱、改进产品。密码产品不适合于互联网免费模式。同时也很认同经济学家熊彼特认为的企业家的创新不是发明新技术，更多的是把新技术转化为商业成果，创新主要在应用层，通过把新技术、新方式把原有的一些生产要素重新组合。这个观点非常适合于密码产业，因为我们是要在现有的基于 RSA 密码体系改造成基于商用密码体系，很多产品和解决方案都是现成可以参考的。比如说零信技术的国密云 WAF 服务，就是这种创新，CA 能签发 SSL 证书，云 WAF 和 CDN 服务需要 SSL 证书，传统方式是用户分别向 CA 和云服务提供商分别购买，并手动实现配置 SSL 证书。而零信国密云 WAF 服务就是基于现有的阿里云 CDN/WAF 打造，把零信云 SSL 系统和云服务系统通过 API 打通组合出一个新的网站安全云服务，让用户一键实现国密 https 加密、WAF 防护、CDN 分发和网站可信认证等四位一体的网站安全防护服务。

另一本推荐的书是高瓴资本张磊的《价值》，这里有一个理念非常好：不能只讲互联网思维，解决用户的痛点，这是需求决定供给的商业模式。实际上，供给引领需求，供给跑到

需求前面在商业世界也是成立的，并且创造新的供给和刺激新的需求的产品一般都有更高利润，这一点值得密码从业者借鉴。我们不能只是不断改进密码产品的“老三样”(密码机、密码卡、USB Key)，而且应该根据用密码来保障互联网安全的需要提供各种创新的产品，不能说起国密改造就是改造门禁系统，应该提供更多的密码产品来刺激新的消费，因为整个互联网安全架构的基础是密码。零信技术的自动化实现国密 https 的国密 HTTPS 网关就是一个这样的产品，彻底让用户从传统的申请 SSL 证书方式解脱出来，实现国密改造的零改造。

最后，王高华建议大家订阅零信任安全研究院公众号，这里的特色栏目是密码讲堂，已经开讲了 5 讲，从什么是密码讲起，可以免费学习密码是如何在保障互联网安全的各个方面发挥重要作用的，这是一个免费的公益讲座，每周一期，以期能为计算机专业人才快速了解和掌握密码知识提供一个学习的课堂，为培养我国奇缺的密码人才做出一点点贡献。王高华总结了一句话：密码事业无限，密码人才奇缺。密码讲堂开讲，助力密码事业。欢迎大家经常访问零信技术官网的 CEO 博客的密码讲座栏目。

请关注公司公众号，实时推送公司 CEO 精彩博文。