受邀 2023 高交会商密展团密码讲座-深度解读《密码法》

大家好！

非常高兴受深圳商密协会邀请在高交会商密展团讲《密码法》。

今天讲的主题是：深度解读《密码法》，大家都知道这次高交会是第一有了商密展团，《密码法》是商密的第一大法，很重要！今天我是从一个密码从业者的角度来讲《密码法》，因为在网上看到很多解读《密码法》的文章，说实话，我自己看得一头雾水，我今天看看能不能把这事讲清楚。

这个副标题是：密码事业真无限，找对方向是关键。今天讲座面向的是咱们密码从业者、或者网络安全从业者，或者大数据从业者，为什么要讲《密码法》呢？因为做大事要先抬头看路，首先看路，看清了方向以后，我们才埋头苦干。方向如果错了，那白努力了。方向对了，跟准方向，这就是跟准大势，那就事半功倍。所以，大方向很重要，学习《密码法》就是掌握大方向，希望大家今天能有收获。

《密码法》总共有 44 条，我今天只解解读其中的 8 条。另外，我会对比讲一下《密码法》和美国《联邦零信任战略》，两者有什么相似之处，比较一下。第三个话题，我会讲商密改造这块，到底应该改什么？如何改？最后，我会总结一下，学法懂法，把握大方向和大机会。这很重要，真的，方向很重要！

首先请大家看一下，去年 2 月 24 号俄乌冲突发生后，发生在互联网的一个安全大事，可能有些同志并不知道。不知道这个大事是什么？看看这个图表，从 2 月 24 号俄乌冲突发生到 2 月 28 号开始，大量的俄罗斯政府网站和银行网站部署的 SSL 证书被吊销，总共有三千多张证书，第三天开始，有大量的证书被吊销。这什么意思呢？证书被吊销以后什么结果？就是网站访问不了了，来看看这个演示网站访问不了的情况。就是政府网站和银行网站访问不了了，天下大乱！这是美国把一个密码产品，一个保证互联网安全的公共产品，作为一个制裁工具来制裁俄罗斯。不仅是禁止使用，证书吊销禁止使用，同时断供。断供什么意思？从 3 月 3 日开始，美国 CA 不再给俄罗斯发证书了。这也是个大事，不仅以前发给你的证书被吊销，用不了了，而且后面不再签发新的证书了，这是个大事。可能大家知道冲突发生后银行系统被禁用及其他制裁措施，但互联网安全的这个制裁也是个大事，导致这个政府网站、银行网站访问不了了，这是个大事。

这事会不会发生在我们国家？如果发生在我们国家，那我们也一样访问不了政府网站、访问不了网银网站，还有微信，大家现在正在看直播，也用不了了。为什么？因为现在我们国家所有网站，99.99%的网站部署的都是美国 CA 签发的 RSA 算法 SSL 证书。就跟俄罗斯是一样的，俄罗斯是 100%，我们国家因为这两年还有些密改，现在有些网站部署商密 SSL 证书了。

再看看这个 PPT 截图，这是我在 2019 年 8 月第七届互联网安全大会上的演讲 PPT，在 2019 年，朋友们，四年前我就提出这个问题：我国所有网站，淘宝、京东、支付宝、微信、银行网站、政府网站、大学等都在用 RSA SSL 证书，我们做好断供和吊销的准备的吗？我们有备胎吗？

当时我提了这个问题，但有的专家说：你这是危言耸听！这些商业 CA 机构怎么可能把证书无故吊销呢？ 同志们，2022 年验证了，这事在俄罗斯真的发生了！俄罗斯就是一个月内被吊销了三千六百多张 SSL 证书，基本上等于我国现在目前政府网站的证书数量。证书被吊销就用不了，真的发生了这事。所以，我们国家就应该未雨绸缪，提前做好准备，以应对可能将来发生的同类安全事件。

所以，为什么我要讲《密码法》？《密码法》高瞻远瞩，未雨绸缪，防患未然。《密码法》是 2020 年 1 月 1 日实施，俄乌冲突发生在 2022 年，在这之前，《密码法》制定者就想到了不能用别人家的密码，别人家的密码是没法保障我国互联网安全的。所以，《密码法》第 27 条要求关键信息基础设施必须采用商用密码来保护。

从发生在俄罗斯的真实案例说明了《密码法》的高瞻远瞩，早就预判了这事会发生！只不过是还没有在我国发生而已，但已经发生在俄罗斯。讲这事，就是想让大家理解为什么有《密码法》这个大法。理解这个很重要，太重要了，涉及到网空安全，是第四安全，海陆空安全、

网空安全都是国家安全。没有网络安全就没有国家安全，这是国家安全！所以这个密码法就叫大法，很重要！国家出台的《密码法》和最近生效的《商用密码管理条例》要求用商用密码来保障关键信息基础设施安全。银行、政府网站、公共服务网站都属于关键信息基础设施，都需要采用商用密码来保护。为什么说 RSA 密码保障不了，因为人家随时可以吊销，甚至断供！会拿这个当制裁工具来卡你脖子，这是卡脖子的密码产品。那怎么办？所以，我们学习《密码法》就是要知道我国网空安全急需用商用密码来保护。哪里需要保护？SSL 证书这块是最关键的，因为它是互联网的一个安全基础设施。

我今天解读《密码法》，解读最重要的是第二条：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。43 个字，第二条把密码说得一清二楚，这很重要。

第二条里面的第一点就是：密码法明确定义了密码的形态。形态是什么？是技术，首先密码是一种技术，叫密码技术。它可以是一种产品，叫密码产品。也可以是一种服务，称为密码服务。密码它是以三种形态存在的，可以是技术、产品和服务，这就给密码从业者指明了方向，就是我们要干什么。干密码这个行业，你到底怎么干？要么研究密码技术、要么研发密码产品、要么提供密码服务，提供密码服务目前一般都是云服务。这个是第一点，讲清楚它的形态。

那第二点？则是明确定义了密码的用途，密码该怎么用？密码到底用在哪？大家看清楚哦，第一个用途是加密保护，刚才大家看了网站的 HTTPS 加密，SSL 证书就是用于加密保护，从浏览器到服务器端的加密保护，加密传输安全，这是最广泛的用途，是互联网安全的基础。互联网发明的时候是 HTTP 明文传输， SSL 证书发明后就能实现从用户浏览器到服务器端的加密保护。只有在实现 HTTPS 加密保护后才有了网银，才有了电子商务，才有了其他各种各样的网上服务。为什么？如果不加密的话，a 给 b 转 100 块钱，明文的话，就可以篡改为 c, 这是不行的。所以，密码的第一个用途是加密保护，这一点必须清楚。HTTPS 加密保护，从用户端到云端的传输加密。数据加密、邮件加密、文档加密、数字签名，都是加密保护。所以，这个是第一大用途，很重要的第一个用途。第二个用途才是安全认证，用数字签名实现可靠的身份认证。

为什么这一块一定要说清楚呢？咱们听众里很多 CA 同行，传统的 CA 业务都只是安全认证，大家知道，就是 USB Key 认证，电子签名。但是，密码的第一用途是加密保护，这个市场是最大的。就是刚才说的 SSL 证书，HTTPS，保障全球互联网安全。从 2013 年开始，10 年全球已经签发了 110 亿张 SSL 证书，SSL 证书是全球用途最广、量最大的一个密码产品，所以，这个产品市场是最大的，密码产品中这个市场最大。我们做密码这块到底做什么？当然做最大的市场。对不对？这是第二条的第二点，第一点是定义形态，第二点是用途。这个用途应该把

握好，不只是身份认证，这是排在第二位的。最重要的用途是加密保护。

第二条第三点明确定义了密码的技术路线，就是国产密码算法。采用特定变换的方法来实现的，这个特定方法就是密码算法，指 SM2、SM3、SM4，还有 SM9。这个讲得很清楚啊，不包括国外的密码算法，RSA 算法不算！只能是用国产密码算法。这点很重要，不能搞错！有人说密改搞了，用 RSA 证书不行！不符合《密码法》定义的技术路线。

第二条第四点很重要，明确定义了密码的保护对象。保护谁？ 那就是信息。这个密码保护的是信息。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。后面还有个“等”字，就是其他元素都需要密码来保护。因为除了信息外，信息等，这里面有“等”。《密码法》是很严谨的，就是这个“等”，包括了所有数据。这就不难理解为什么《数据安全法》《个人信息保护法》都明确说了必须用密码来保护个人数据和个人信息安全。这个是大家要理解的。

所以，在第二条里面我解读了 4 点，很重要 4 点。包括标点符号才 43 个字，能解读这么多信息出来。很重要，所以先解读第二条。

接着解读一下第六条、第七条和第八条。第六条是国家对密码实行分类管理。密码分为核心密码、普通密码和商用密码。核心密码、普通密码是保护国家机密的。商用密码是保护不属于国家秘密的信息，公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。所以，今天讲的都是商用密码，我们这个展会就是商密展团。大家有时叫国密，国密 SSL 证书、国密浏览器，都是不规范讲法。正式术语应该是：商密 SSL 证书、商密浏览器、商密 HTTPS 加密。

再说一下第 21 条，写的很清楚，国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。这是商用密码市场体系建设，促进鼓励发展，这给我们指明了方向。鼓励大家去研究、研发，鼓励大家学习交流。鼓励大家产业化，高交会，就是要成果转化，鼓励的。必须有一个有序的市场竞争体系，才能保证产业健康发展。

第 27 条，这个更重要。第 27 是什么？法律、行政法规和有关规定要求使用商用密码进行保护的关键信息基础设施应当使用商用密码进行保护，可理解为必须的，这对密码企业和用户都非常重要。为什么呢？因为对密码企业来讲，所有关键信息基础设施都必须用，市场很大！这是一个很大的市场！那么，哪些属于关键信息基础设施？依据 2021 年 9 月 1 日施行的《关键信息基础设施安全保护条例》第二条，写得很清楚，关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防工业等这些都属于关系到国家安全、国计民生，都属于关键信息设施，它的范围是非常广的，都需要商用密码来保护，这个市场很大！

如果违反了第 27 条呢？第 37 条写的很清楚，未使用商用密码，或未按照要求开展商用密码应用安全性评估的，怎么办？罚款 100 万，主管领导罚款 10 万，这个厉害！所以说，这个是咱们密码企业做市场的尚方宝剑！同志们，一定要利用好这个尚方宝剑！必须做国密改造，商密改造，否则违法！

OK，那问题就来了，到底哪个系统需要商密改造呢？该如何改造呢？现在这个市场很乱，到底要改造什么？门禁改造很流行，因为它也可以得分，并且很容易改造。大家不知道应该改造什么，我今天要给大家讲清楚。讲清楚为什么需要改造？什么需要改造？这很重要。哪些系统需要改造？很重要，一定要清楚。

先对比一下美国的《联邦零信任战略》，去年 1 月 26 日发布。零信任战略保障身份安全、设备安全、网络安全、应用安全、还有数据安全，五大支柱。网络安全这块，第一个是 DNS 安全，DNS 必须加密，加密 DNS，因为 DNS 是互联网访问的基础，很重要。我国 DNS 现在基本上都是没加密的。零信任战略中讲的 DNS 加密是 DNS over HTTPS, DoH，还有 DoT, 就是 DNS over TLS。为什么是这个呢？因为 DNSSEC 效率很低，是已经很落后的技术了，被抛弃了。所以，大家都用 DNS over HTTPS，一个 SSL 证书的应用。

第二个要求就是 HTTPS 加密，加密 HTTP 流量。要求所有.gov 网站，政府的所有网站强制必须走 HTTPS。而为了防止有的政府机构没有强制 HTTPS，怎么办？跟浏览器合作，预置.gov 域名只能用 HTTPS 协议访问。要求浏览器访问.gov 域名的网站不能用 HTTP 协议来访问，只能用 HTTPS 协议访问，这是有一个闭环管理措施。这个非常非常厉害。现在我们国家很多政府网站已经部署了 SSL 证书，但是实际上没有强制实现 HTTPS 加密，等于没有部署一样。还是可以用 HTTP 明文访问，这个不行。这块值得学习。

第三个流量是一个邮件加密这块，必须实现 TLS 加密。所以，我们总结一下这个零信任战略有五大安全目标，身份、设备、网络、应用、数据安全，都需要靠密码、靠 PKI、靠证书来实现身份认证、数字签名和加密。HTTPS 加密、DoH、DoT、TLS 加密，是核心。所以，这个对我们密码产业的启示是什么？这个零信任模型五大安全目标全部用密码来保证它的安全。这里面每一个方案都是一个很大的市场，所以才称之为战略。零信任的安全目标不只是身份认证，我刚好顺便纠正一下。零信任有五大应用，其核心是密码的全面应用，不只是身份认证。核心是密码的全面应用，这里面商机无限！重点是 HTTPS 加密。所以，商密改造的重点应该是 HTTPS 加密。

这就是为什么我刚开始时引用俄乌冲突的安全事件。为什么需要商密 HTTPS 加密？是密码合规的需要，等保密评需要，是合规需要，这是第一个需要。第二个是保障关键信息基础设施的不间断服务的需要。我刚才讲过俄罗斯的真实案例给大家看，中断了服务。因为你用的是

人家的密码产品来加密的。中断了，断供，你用不了了。所以，合规是为了保证关键基系统的不间断的服务的需要。《密码法》要求合规，到底商密改造首先改什么？当然是 HTTPS 加密改造！这是互联网的基础安全。这个被人家掐脖子了，必须把先把卡脖子问题给解决了。当然，门禁改造有用，但不是卡脖子的。卡脖子的是 HTTPS 加密，让网站访问不了，微信用不了！这才是卡脖子的问题，我们必须把这个先改了。所以，我需要先讲清楚为什么需要 HTTPS 加密？有两个理由：一个是合规。现在很多市场驱动都是合规，我上次在一个讲座中打了一个比方，合规就像咱们知道的“开车不喝酒，喝酒不开车”是一样道理，为什么要你开车不喝酒呢？这当然是交管合规，合规需要。但是，它真正的目的是为了保证你的自身安全，为了保命！为了保命，这是对你自己有好处的事情，不要仅仅是为了合规。

所以，为什么需要商密 HTTPS 加密的理由有两个：一个是《密码法》合规，第二个是为了保证自己的业务系统能不间断地为用户提供服务。这是一个认识高度问题，如果你的高度到了，认识到重要性。如果你认识不到，你就是被动合规。认识到了，那是主动合规。只有主动合规，你才有动力去把你的业务系统改造好。为什么呢？因为你的系统太重要了，你不能让它停顿了。所以，你要去改造，去做商密 HTTPS 加密改造。为什么我在前面铺垫那么多呢？说是想让大家理解我们到底需要改造什么的问题。这一点我们一定要认识清楚。

我们看一下整个互联网的安全，目前是基于 RSA 密码体系来保障全球互联网安全的。云端有 SSL 证书，实现 HTTPS 加密，这个最重要，这是关键。因为互联网，那么复杂也不复杂，就两端，不仅有服务端，还有一个客户端，两端之间的信息交换全加密，必须加密。怎么加密？用 SSL 证书实现 HTTPS 加密，这个是重点。还有客户端证书用于身份认证，我怎么证明我的身份？就用客户端证书做身份认证。当然，现在有很多身份认证方式，除了客户端证书以外，还有刷脸认证，用户名/口令认证。而最安全的认证方式是用证书方式，密码的安全认证用途。

整个互联网上，从云端到客户端之间跑的各种文档，它们也需要证明其可信身份。你在网上看到一个声称是公安局的文件，有个图片红章，能信吗？不能相信，必须有数字签名。只有数字签名才能证明它的可信身份，因为数字签名是不可篡改的。证明了它的身份，才相信这是真的政府文件，防止上当受骗！代码安全这块，网上跑的代码，如果没有数字签名的话。这是什么概念？有一个加油站被黑，被木马勒索，为什么？因为它在网下载升级软件包没有数字签名，并且是明文下载，下载的文件被篡改了，变成了木马进来了。木马收到以后，系统也不验证有没有数字签名就安装了，装了就完蛋了，机器被锁了，被勒索了。万物互联，互联网服务需要代码，需要你运行代码，运行之前需要验证数字签名，验证代码的合法身份。通过 HTTPS 加密通道下发代码和验证代码，才能保证万物互联的安全。

这是整个目前全球互联网的架构，全是密码在起保障作用。所以叫公钥基础设施，

PKI(Public Key Infrastructure)。什么叫基础设施？水电气，这就是互联网的水电气，这就是密码的作用。最重要还是 HTTPS 加密，数据从客户端到服务端的加密。因为互联网只有两端，HTTPS 加密是最最关键的。

我们国家必须用商用密码体系 PKI 来保障互联网和万物互联安全。怎么保障？一样的架构，但采用商密 SSL 证书来实现 HTTPS 加密。采用商密算法的客户端证书来实现身份认证。采用商密算法的文档签名证书来签名文档，证明文档身份。采用商密算法的代码签名证书来证明软件代码的身份。国产操作系统的所有代码的安全，要保障国产操作系统的安全，必须要有代码签名，证明代码的合法身份。所有物联网设备要升级软件，包括车联网。今天就有一个车联网密码应用论坛，有一个专家的演讲就讲到了升级软件包，必须有数字签名，否则就会下载一个木马，恶意攻击代码。这个很重要！它是保证互联网、万物互联、包括车联网安全的。当然，一样的，它的核心是 HTTPS 加密，这是一个核心。

现在已经是大数据时代，大家知道数据是核心，数据很重要。《数据安全法》定义的数据的七个生命周期：数据收集、传输、提供、使用、公开、加工、存储，整个七个生命周期里面，最重要是数据传输。每个生命周期都用密码了，数字签名，时间戳，加密，密码保护数据安全。核心是什么？数据是要流通的，数据不流通不交换，就没有它的价值。最重要的是什么？是在六个环节里面的数据流通中的 HTTPS 加密！ 这个绝对是最关键一个，其他方面做得再好，如果你不采用 HTTPS 加密的话，数据在流通过程中泄露了，
被别人窃取了，被别人篡改了，其他做的工作都毁于一旦！因为 HTTPS 加密是基础，很重要！

总结一下，解读《密码法》，《密码法》第二条说的很清楚。《密码法》第二条定义的密码是用于加密保护和安全认证的，采用商用密码算法，提供密码产品和密码服务。提供产品服务干嘛用呢？为了保障五大零信任安全的，保证设备的安全，保证身份的安全，保证网络的安全，包括 DNS 安全，HTTPS 加密、邮件加密 TLS、应用的安全，文档的安全，数据加密，数据的安全。HTTPS 加密是核心。所以，《密码法》加上《电子签名法》、《网络安全法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》，
这些就是我们国家的零信任战略，中国的零信任战略！对没有采用密码保护的系统零信任，没有密码不信任！普及商用密码应用，保障关键信息基础设施系统安全！这就是为什么我介绍了美国联邦零信任战略，零信任战略的五大支柱。我国也有零信任战略，就是《密码法》，一个能够媲美的战略，没有采用密码保护的系统就是不信任，这就是零信任！

下面我讲一下如何实现 HTTPS 加密的商密改造。HTTPS 加密是最重要的，这必须首先改造，因为这是核心安全。如何改造？我看到一个招标，就是向 CA 买一张国密 SSL 证书，Web 服务器改造支持国密算法，并安装国密证书，再买一个国密浏览器。浏览器这个话题有意思，

后面讲。这个改造方案可行吗？答案是不行的，但是都是这么干的！

为什么不行？因为目前大家买的商密 SSL 证书如果不支持证书透明，是无法保证 CA 机构的证书签发行为的。证书是否是用户自愿申请的？无法保证证书是否是恶意签发的。所以，国际上从 2013 年到现在，全球签了 110 亿张 SSL 证书全部都支持证书透明。国密 SSL 证书也应该这样，这是其一。第二，Web 服务器改造，只有 Nginx 支持国密改造。但是大量的服务器，如 IIS，IMB 服务器等都是没法改造的。那怎么办？买了国密 SSL 证书也没用，还是实现不了国密 HTTPS 加密！这是第二个方面的不行。

第三？买个国密浏览器可行吗？我看到的那个标是一个上千人的单位，只买十个浏览器许可，有意思吧！我觉得这就是用户的无奈之举。没办法，因为要过密评，必须干。这就是为什么零信技术要推出完全免费的国密浏览器！要普及商密算法，普及商密应用，普及商密 HTTPS 加密，没有免费的商密浏览器，是不可能成功的！全球互联网为什么能够实现全覆盖 HTTPS 加密？那不就因为谷歌、微软、苹果、火狐都有完全免费的浏览器？国密也是一样的，很重要，必须有完全免费的国密浏览器！这一点我觉得应该要补充说明一下，这个很重要！

如何实现商密改造？大家都可能知道，商密改造难，很难！难在哪里呢？难在现在的所有系统都是基于 RSA 密码体系建立的，人家这个体系已经成熟运行 30 年了，40 年了，就像深圳市成立四十多年了，整个城市的供电供水系统，全部水管给它换掉，容易吗？不可能！所以，太难了！因为整个生态架构都是基于 RSA 密码体系的。

那怎么办？有哪些难点呢？有六大难点。浏览器不支持国密，Web 服务器不支持，传统 CA 系统不支持签发国密 SSL 证书，CDN/WAF 不支持国密，大网站离不开 CDN 和 WAF。改造工程复杂，无从下手。改造有很大的风险，很多业务系统不能动，难就难在这里。为什么国密改造难呢？就难在这里，把体系改掉太难了。

刚才说的 HTTPS 加密这块，传统的模式就是向 CA 申请 SSL 证书，把 SSL 证书装到服务器上就完事了。为什么这么简单呢？就因为整个体系都已经支持国际算法了。但是国密就不一样，改造那就难了，要改造整个生态。难，怎么办呢？

我们有一个解决方案，一个商密 HTTPS 加密自动化解决方案。这个解决方案就是把浏览器换成国密浏览器，免费的。Web 服务器没法改造，改造太难了，那就不改造！我们的方案叫零改造，零改造实现国密 HTTPS 加密，自动化实现！干脆不改造，在外面加一层商密来保障。这是一个端云一体的解决方案。有“端”有“云”，“端”就是网关。具体细节明天再讲，提前透露一点,就是国密 HTTPS 加密自动化网关，就是在 Web 服务器前面加一个网关，你的服务器不用动，不用申请 SSL 证书。证书从哪里来呢？通过端云一体，通过云上的云 SSL 系统，还有证书透明日志系统、自动化证书服务系统，自动化配置商密 SSL 证书和国际 SSL 证书，双证书

自动化配置，自动配置双证书来实现自适应算法的 HTTPS 加密。这是一个自动化的解决方案，零改造，原服务器是不需要改造的，零改造自动化实现商密 HTTPS 加密！

最后总结一下：《密码法》给我们指明了方向，密码技术、密码产品和密码服务。也给我们的指明了用途：信息加密和安全认证，每一个密码从业者要想一想到底做哪块，什么是最有前途的？密码最大市场在 HTTPS 加密，HTTPS 加密保障全球互联网安全。因为每一个网站、每一个系统、每一个应用都需要 HTTPS 加密，这才是最有前途的一个事业。所以，这个是方向很重要。学习《密码法》，抓住密码大商机！大家一起努力，打造密码产业新高地！

总结一下，《密码法》就是零信任，零信任加密码，加云计算，端云一体解决方案，等于网络安全的未来！密码，是非常有前途的一个产业，大家要把握这个大商机。

今天就讲这么多，谢谢大家，希望对大家能有所帮助。

王高华

2023 年 11 月 16 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。