2023 高交会商密展团零信展位密码讲堂-数字证书、SSL 证书

大家好！

前天和昨天我在高交会商密讲座讲了《密码法》，反响还不错！为什么讲《密码法》？那是要抬头看路，看清楚方向，知道干什么。今天，就开始讲埋头拉车的内容，讲密码的重要应用，PKI、数字证书、SSL 证书，今天就讲这个具体的内容。

有八项内容，第一就是讲 PKI、公钥、私钥、加密、签名，接着讲 PKI 如何保障全球互联网安全，重点当然讲 SSL 证书，这是最重要的一种证书，因为全球现在已经签发了 110 亿张，从 2013 年十年时间签了 110 亿张，这个厉害。也要讲商密 SSL 证书、SSL 证书分类、可信根认证计划。讲浏览器是如何验证 SSL 证书的，为什么信任这张证书。最后，讲一下零信浏览器有哪些优势。这些都与 SSL 证书相关，今天讲的内容还挺多的。

那什么是 PKI？PKI 就是公钥基础设施，英文叫 Public Key Infrastructure，不是 KPI 绩效考核，是 PKI，它是互联网安全的核心技术，很重要。所以，后面还会解释为什么叫公钥基础设施。什么叫公钥和私钥？要理解 PKI，得先讲这个。在密码体系里面，有对称加密和非对称加密两种方式。对称加密很容易理解，就是对称的，就是一把钥匙开一把锁，你用什么加密的，就用什么解密。有什么好处？就是效率很高。但是，对称加密有一个问题，如何把这个密钥安全地传给对方，因为大家都必须用同一个密钥，我用一个密钥加密，必须把密钥告诉你，用这个密钥来解密，这里就有问题了。大家在日常工作中应该用过 Word 文件加一个口令，那么，加完口令后，你通过微信把 word 文件发给对方了，这个口令怎么给？我经常在讲课时问大家

这问题，你们怎么把这个口令告诉对方呢？回答是也用微信发给他，那有什么用？如果文件被窃取了，口令一样会被窃取，那加的口令就没用了。

所以，实际上，这个公钥怎么交换，怎么给人家，是个问题。特别是计算机互联网这块的密钥交换，不是人工交换，你不能这样使用同一通道传递密文和密钥，这是肯定不行的。所以，RSA，美国的三位密码专家，三位专家的名字第一个字母合起来就是 RSA，RSA 三位专家发明的一个算法就是非对称加密算法，它是两把钥匙，把密钥拆成两份，简单讲，一份是公钥，一份是私钥，两把钥匙，有一把钥匙是公开的，叫公钥，有一把钥匙是不公开的，只有你拥有，叫私钥，这个问题就能够解决了。那公钥如何分发？公钥如何告诉你？怎么干呢？很巧妙。大家看看这个图，明文是一只棕色的狐狸迅捷地越过那只懒狗，这是 ABCD 26 个英文字母打字练习用的一句话，这是明文，我使用收件人的公钥，公钥是可以通过各种渠道拿到的，大家可以分发公钥。我用公钥给你加密，变成密文。密文就可以通过互联网传输了，不怕，变成乱码了，大家看到是乱码。对方收件人收到密文后，用私钥解密，就把密文变成明文了，这是一个非常好的机制。所以，你只需要有一个公钥交换机制。对于邮件加密来讲，公钥怎么交换？我发一个签名邮件给你，就把公钥带过去了。或有一个公钥库，像 PGP 加密，有一个公钥库系统，我去搜一下你的公钥是什么，我拿下来用。就是云上有个公钥管理库，可以去取。有很多方式可以交换公钥。其实，SSL 证书，那就是公钥，你用浏览器 https 访问网站，就能返回公钥给你。所以，公钥是需要有交换机制的。

这是加密，签名则是反过来的。这是学密码，用密码，从事密码行业都应该理解这个基础东西，必须知道。不知道的话，你就没法跟客户讲清楚，如果你把这个跟客户讲清楚了，客户会认为你是专家，同学们，这很重要。加密就是这样实现的。签名呢？签名是反过来的，我有私钥，只有我拥有，我用我的私钥给这个文件签个名，再发给对方，当然发给对方时候同时把公钥带上，带上公钥，对方收了我的签名后，就可以验证我的签名，用公钥去核对，用算法一算，确实是对的，就验证通过了，就能证明身份。这个身份确实是我，这个签名确实是我签的，它叫数字签名。是用公钥去验证，这是两个不同的用途，两个最重要的用途。这个一定要搞清楚，这两个用途一定要搞清楚。为什么呢？因为这是密码的核心，不管是国际密码算法还是商用密码算法，都是这个原理，这是基础，我们密码从业者一定要知道。一定要知道什么是加密和签名，大家应该能理解这个，我这个比较简单的解释，应该能理解。

那什么是 CA 呢？我现在有公钥给对方，但如何证明这个公钥是谁的呢？需要一个中立的第三方，大家信任的，用他的私钥给这个公钥签名，有点绕，这个第三方就是 CA 机构。 英文 Certification Authority, 权威机构，你认可我给你的签名，你如果验证了签名没有问题，那你应该承认这个签名确实是我的签名。这是一个公钥基础设施，用来给公钥签名的系统，叫 PKI

系统，叫公钥基础设施。再加上证书颁发系统、证书管理系统，就叫 CA 系统，就是签发证书的系统。PKI/CA 系统签名后的公钥就叫数字证书。为什么叫证书呢？因为数字证书中含有公钥基础设施认证过的身份信息，能有效证明这个公钥的可信身份，所以叫做数字证书，以区分传统的纸质证书。这个就是数字证书。

数字证书一般分为三类，也有分四类的，我喜欢分为四类。为什么？我认为互联网安全需要这四类证书， 第一类就是 SSL 证书，第二类是客户端证书(邮件证书)，还有一类是代码签名证书，还有文档签名证书。SSL 证书，后面会详细讲。先看看代码签证书，左边这个图，我刚刚装了微信软件，右键查看属性，有一个数字签名的属性，显示是谁签名的，这就是代码签名证书。而邮件证书，大家看 Outlook 里如果有数字签名会显示，数字签名层会显示签名信息。看第二个图，会显示这个邮件已经含有数字签名，会告诉你谁签名的。那文档签名呢？零信浏览器能实时验证文档数字签名，点开签名属性，能看到这个文档签名，文档签名证书有效。这 4 种证书用于保障全球互联网的安全，所以叫公钥基础设施。

核心的是从客户端到服务端的连接安全，这是 SSL 证书在保证的。现在的服务端就是云端，客户端就是浏览器或手机 APP，浏览器连接到云端，连接安全靠 SSL 证书来实现 HTTPS 加密，这个是重点，这个连接不安全，其他任何安全都是白搭，都是空中楼阁，其他安全措施都没用。现在进入了云时代，但是目前大家防护理念还是城堡理念，大家投资了很多安全防护设备，在云端部署防护，防护云端服务器，这没有问题，是需要防护。但是，忽略了现在是数据时代，数据是要流通的，数据怎么流通？从云端/服务器端流到客户端去，但是，如果你不用 HTTPS 传输加密，没有部署 SSL 证书，是无法保证数据流通过程的流通通道安全的。可以说你的堡垒防护是没用的，为什么呢？因为你的系统已有防护，攻击它太费劲了，怎么办？
那就不攻击它，而是等在路上，在数据从云端到用户的路上等，你数据过来，没有 HTTPS 加密，是明文，就可以轻松拿走。同学们，因为互联网的连接经过了太多的路由了，每一个路由都能看到你的数据，如果不加密的话。所以说，HTTPS 加密是最重要的一个数据安全保护措施。

现在是数据时代，防护观念必须改变，既要保护云端服务器的安全，又同时要保证数据通道的安全，要把数据安全地流通到用户端，流通到整个生命周期里面去，否则你的云端防护再安全也没用！因为数据出去以后是明文，被人拿到了，你的防护有意义吗？你防护的目的是为了你的数据安全，那是你的客户数据，你的基础业务数据，很重要，重要数据就这样被窃取了！所以说，这个 HTTPS 加密是保障互联网安全的基础，基础安全！

通道加密以后，通道上的代码不能随便运行，需要代码签名，保证代码的身份。很多攻击，前段时间一个加油站被勒索，那当然，你会说这是传统的安全防护做得不好，实际上它不是这

么简单，但又是很简单的事情。为什么这么说？就是系统升级代码没有数字签名，升级代码的通道是从云端下载下来，没有走 HTTPS 加密，别人就有能力把你代码给改了，没有 HTTPS 就可以给改了，换成他的木马了，换成他的软件了，他软件没有数字签名，他的代码到了设备后，你设备不验证数字签名就安装了，就被他挟持了，你系统就被他干掉了！所以，大家知道了吧，HTTPS 通道加上代码签名，就这两个事就能保证你的设备安全，升级安全！不需要你的终端设备搞一堆几十万的防护，没用！再说，物联网设备根本做不到，算力不够，没法做这个！没有地方可以装这几十万的防护系统，也没有任何必要！

所以，PKI，密码是一个很简单的解决方案，能搞定这个事！但是，传统的安全防护就是卖一堆东西给你，根本没用！实际上，你通过加密通道下发有数字签名的代码就 OK 了！另外，设备端验证这个签名是否可信，是不是你要的软件，查验代码的签名是否正确，PKI 能保证代码没有被篡改！这个厉害，所以 PKI 是很厉害的东西。技术搞错了，真的是白花钱，还没保证安全，照样被黑掉！

这是代码签名，还有文档签名也很重要。现在所有文档都在互联网上跑，两端的中间跑的是代码和文档，需要代码数字签名，文档需要数字签名。为什么需要数字签名？因为文档现在都是电子化，文档 PDF 或 OFD，如果没有数字签名，它说它是政府公文，某某单位的，有一个橡皮章图片，你信吗？很多诈骗就是这样干的，那问题出在哪里呢？ 问题是在文档发布方，没有给这个文档做数字签名！如果文档有数字签名的话，他是不可假冒的，假冒不了！为什么不可假冒？因为发布者身份是第三方可信 CA 验证身份的，操作系统信任的这个身份，是可以保证这个文档身份的。

所以说整个互联网，别看互联网那么复杂，就只有云端和用户端，中间跑代码，跑文档，客户端就用 CA 签发的 USB Key 证书证明身份，证明你身份是可信的，没有问题。服务端用 SSL 证书保证它的身份，也保证传输加密了。代码和文档也有签名，整个互联网就安全了！这就 PKI 的作用，同志们，这就是 PKI 的作用！这就是为什么叫公钥基础设施，它是互联网的安全基础设施！就都是靠它，PKI，数字证书是保障互联网安全的，很重要！

今天重点讲 SSL 证书。这是基础通信安全，大数据流通的基础安全。SSL 证书，大家用 Windows 证书查看器打开，很有意思，它会告诉你，有两个作用，既是客户端又是服务器端，向远程计算机证明你的身份，保证远程计算机的身份，就是保证服务器的身份，它是有两个作用的。实际上，SSL 证书就是这样的一串乱码，2048 位的证书。这就是 SSL 证书，刚才讲了为什么重要。整个互联网从 2013 年有证书透明开始，10 年签发了 110 亿张，所以，SSL 证书是全球第一大密码产品啊！我在讲《密码法》讲座时也说了，大家一定要搞清楚，搞密码，不要全部集中在做密码机、密码卡、USB Key 证书，那些都是边缘产品！我估算过，全球这 110

亿张 SSL 证书的签发，只需要目前大家做的密码机，两台，一天就给你签出来了！现在签了 10 年，才签了 110 亿张证书，要那么多密码机干嘛？所以，密码机是严重过剩的产品！

同志们，最大的产品就是 SSL 证书这个产品，SSL 证书的应用！所以，为什么美国 CA 只干这个，这个是互联网安全的关键产品！互联网安全基础设施！我们国内 CA 基本上都在做客户端证书，应该转型！因为互联网的安全，基础通信安全，就是 SSL 证书！SSL 证书厉害，厉害在哪？厉害在俄乌冲突，美国把它当武器用！当制裁工具啊！同志们，重不重要？因为它是保证数据安全的！从 1994 年 NetScape 发明 SSL 证书以来，一直在使用，发展最快。

我先讲一下 SSL 证书，还要讲国密 SSL 证书，又叫商密 SSL 证书。现在大家都在用 RSA SSL 证书，或 ECC SSL 证书，这个体系是美国控制的。在俄乌冲突发生时，美国 CA 把俄罗斯网站 SSL 证书给吊销了，把 SSL 证书当作制裁工具了。所以，在我们国家，这是一个巨大的安全隐患！所以，《密码法》高瞻远瞩，要求用商用密码来保护。需要用商用密码证书，商密 SSL 证书。国密 SSL 证书是不规范的说法，规范叫法叫商密 SSL 证书。所以，这个证书你们看，里面名堂很多，不仅仅是算法。我上次给 CA 有一个讲座也说过，RSA SSL 证书我们已经错过了，错过了，不是错了！不能再错过了商密 SSL 证书，不能再错过了！为什么错过了呢？因为那不是我们说了算，别人家的密码算法，别人控制这个市场。所以，这是密码算法问题。

还有，证书是谁签发的很重要，谁签发谁就有权吊销，证书是我签发的。大家都在用免费的 Let's Encrypt, 免费的，干嘛不用？但是，你用了，他就能控制你。他签发的，他就能吊销你证书，让你用不了！网站访问不了！所以说，SSL 证书是一个很重要的产品，这个产品太重要了！我给大家切一下屏幕，看看 SSL 证书是什么样子的。咱们看一下高交会网站，这是 RSA SSL 证书，看一下，大家看到上面有把锁，浏览器会提示连接已加密，再点开，证书有效。这是加密算法，RSA 的。零信浏览器还会提示一个证书透明，这个明天会讲。SSL 证书这把锁，就是起到加密保护作用。

那什么是国密 SSL 证书？看一下湖南省政府门户网站，零信浏览器有个 m 标识，这表示是国密加密的，商密合规，密保合规，用商密算法实现 HTTPS 加密，所以，你点这把锁的话，显示“连接已加密(SM2)”，这是两种 SSL 证书，都有一把锁来表示连接已加密。

我再切回到我的 PPT，讲 SSL 证书到底有那几种类型，SSL 证书有 DV、OV、EV，还有 IV，DV 就是 Domain Validated，只验证了域名。OV 就是 Organization Validated，验证了机构身份。EV 就是 Extended Validated，扩展验证，更加严格的验证。那么 IV 呢？Individual Validated，就是验证了个人身份。这个证书用得比较少，这个是 IV，我是很自豪的！IV 标准是我在 CA/B Forum 上提出来的,因为很多德国的客户，用个人身份来申请 OV SSL 证书，这个 O 字段没法

反映出这是个人，姓名在 O 字段，德国很多公司的公司名称跟个人姓名没法区分，因为 O 字段是用于显示单位身份信息，而个人身份的信任级别应该是不一样的，都写在 O 字段不行。所以，当时我在 2016 年 CA/B Forum 国际会议上提了一个提案，就是给 IV 证书加上 G 和 SN 字段，不用 O 字段，区分一下。这当然是很自豪的事，修改和完善国际标准。

看一下这个截图，左边这个图，这是 OV，一张比较老的证书，大家看看，2006 年签的证书，一张 OV SSL 证书。右边就是 DV，是 GeoTrust 的 DV SSL 证书，Domain Control Validated，只验证了域名。最早的证书只有 OV SSL 证书，刚才我讲过，证书是要验证身份的，验证了你身份，你的身份信息就要写到证书里面去，默认证书就是 OV SSL 的，证书开始就是 OV SSL 证书。但是，大家知道，验证身份需要人工处理，需要查第三方可靠数据库来验证，人工处理是需要时间的，因为以前国际上只有 VeriSign 一家 CA 签发 SSL 证书，可能需要 5 天到 10 天才能拿到证书。所以，GeoTrust 就发明了这个 DV，只验证域名，机器验证，验证码给你，你贴上去，通过验证，证书就自动发给你了。这一下子不得了，是 DV 把 SSL 证书带火了，马上能签发。所以，GeoTrust 只用了两年时间拿到全球第二市场份额。他们发明的 DV 证书问题在哪里？没有身份信息！问题就在这。但是，它做的贡献是让大家都能很快拿到证书。

那为什么出台 EV 证书呢？因为这个 DV 证书普及以后，谁都可以拿到，而以前只有很可信的网站才有证书，如银行网站、政府网站。而现在，DV 证书出来了，欺诈网站通过验证域名就可以拿证书，大量的欺诈网站，假冒银行网站都有证书了，都有那把锁，这下完了，以前大家教育市场是看到锁就是可信网站，看到这个锁就是安全的，所以叫安全锁。我现在改叫加密锁了。现在碰到个欺诈网站，一个假冒银行网站，也有证书， 也有那把锁，怎么办？所以，国际标准就得区分一下，出来个 EV 证书，叫 Extended Validated, 扩展验证，就是必须严格验证网站身份，再签发这种类型证书，为了区分这种证书跟 DV/OV 不一样，浏览器地址栏变成绿色了，这是 17 年前的事情，地址栏颜色变了。大家以前用 IE 浏览器，能看到很多银行的网站地址栏是绿色的，看这个截图。这个很老的 IE，如果没有卸掉的话，还能看到绿色地址栏。所以，它是个发展过程，从 OV 证书开始，到 DV 证书，DV 证书出问题了，就搞出这个 EV 证书出来。很可惜的是，这个 EV 证书，谷歌浏览器，作为一个 70%以上市场份额的领导者，现在认为 EV 证书没用，加密就够了，DV 证书就够了，所以，他把 EV 证书的那个绿色地址栏不显示了，其他浏览器也不显示了，目前只有零信浏览器还在显示这个 EV 证书绿色地址栏。

看看右边这个图，这就是 IV SSL 证书，看看有什么不同吗？IV SSL 证书多了两个字段，G 就是 Given Name,你的名字，还有 Surname，就是 SN，你姓什么，它没有 O 字段。它用 G 字段和 SN 字段替换了 O 字段来展示你的姓和名，这样就可以区分了，原先的 O 不能区分到底是公司还是个人。这里面当然有 OID 可区分，四种证书国际标准都有不同的 OID。国密标

准也会有 4 个不同 OID 来识别，而不只是看证书内容。而因为 DV，OV，EV 在谷歌浏览器都只是显示一把锁，没有什么不同了，所以，现在 DV 市场份额是 83%，OV 16%， EV 只有 0.06%了。都是一把锁，大家就都用 DV 了。最新的版本，就上周更新的谷歌浏览器版本，锁都没有了，因为那把锁没用了，DV/OV/EV 都是锁，没什么意义了。干脆锁也没有了，现在变成了一个 Tune, 两个小圆点加杠。没有这个锁标识了，只有两种标识，如果有 Tune 就是加密，没有这个标志就是没加密，会显示“不安全”，两个状态。谷歌浏览器认为 DV/OV/EV 没有不同了，UI 再区分就没有意义了。

我们了解证书类型后就要讲可信根认证计划了。刚才说了 SSL 证书，如果没有浏览器信任，是没有任何价值的，谁都可以用 OpenSSL 一句命令签出 SSL 证书，但没用，浏览器不信任，会警告。所以，四大浏览器，谷歌、微软、苹果、Mozilla(火狐)都有自己的可信根认证计划，这个图片是 Windows 的信任根，

Windows 里面有个受信任的根证书颁发机构，有个列表，这里列表有 100 多个根证书。四大浏览器都有自己的信任列表。你签的 SSL 证书浏览器是否信任，需要你找浏览器去申请预置信任的。你要分别找这 4 大浏览器申请，申请前提当然你必须通过 WebTrust 审计，再去向四大浏览器申请预置根证书信任。中国的 CA 去申请的话，3-5 年，5-10 年，有可能永远不行！但国际其他 CA，可能很快一个月都有可能，他们说了算。

零信浏览器也有可信根认证计划，我们处理国密根证书预置申请，CA 机构向我们申请，如果我们检查和测试没问题的话，可能一周就给预置发布了，全世界最快，为什么？因为你有工信部和国密局 CA 牌照，只有你签发的证书没有问题，我们就可以马上预置信任。当然，如果有问题的，对不起，就不行。现在，就有一个 CA 来申请预置，被我们拒绝了，因为签的证书有一堆问题，这个不行。虽然国密 SSL 证书标准正在制定中，但是我们是参考国际同等标准的，只是算法换了，要求 CA 同等国际标准来签发国密 SSL 证书，如果你签的证书有问题，我们是不会给你预置信任的。这个要求，正好趁这机会给大家说一下。因为有些 CA 可能有意见，对不起，我们不会像有些国密浏览器什么都不管，只要来申请就给你信任，我们不能这样。CA 会说，为什么某某浏览器预置了，为何零信浏览器不能预置信任呢？对不起，他有他的标准，我们有我们的标准，他标准很低，那是他的事，我们不会采用很低的标准，我们要保护用户安全！

现在，零信浏览器已预置信任 14 家国密 CA 根证书，欢迎还没有预置信任的 CA 机构申请预置。同志们，没有认证的话，一定要抓住这个机会，因为将来的市场，不是 RSA SSL 证书，这只是一个现在的存续市场，而未来市场都是国密 SSL 证书，我们要提前行动，抓紧进入这个市场，进入这个最大市场，商密 SSL 证书市场。所以，抓紧，如果你们做了国密根，抓紧

来申请预置信任。这就是信任根计划，浏览器都有的信任根计划，包括操作系统也有这个计划。

下面，我们讲一下浏览器是如何验证 SSL 证书的，这个很重要，你这个证书有问题的话，会影响用户网站安全的，影响用户访问的数据安全的，没有起到加密作用是不行的，所以，浏览器要很严格的验证标准。我今天会讲，浏览器会验证 9 项，如果浏览器不做这些验证，如果浏览器不做今天我说的这些验证，它就不是浏览器，它就是个废物，没用，根本保证不了你的安全，传输安全。

那第一个验证是什么？如果网站没有启用 HTTPS 加密，只是 HTTP 网站，那浏览器一定会显示“不安全”，现在所有浏览器都是这样的，为什么不安全？因为你从浏览器输入信息到服务端传输过程中没有加密，必须要加密来保证传输安全。所有浏览器都是不信任的，显示“不安全”，这是第一种情况。

第二种情况就是域名不匹配，我们经常碰到，证书是签发给 a 域名的，但是你部署在 b 域名网站上，那就不匹配，它就会有警告，提示“域名不匹配”，这是第二个错误警告。

那第三个呢？就是根证书不受信任，未预置，浏览器不信任。不信任的话，也会有警告，这是肯定的，100%，浏览器都会提示“不安全”。

第四个是证书被吊销，如果被吊销了，会有警告的。为什么会被吊销？有各种情况，如果系统被黑，私钥泄露了，有可能把证书给偷走了，就可能用于假冒网站或解密加密数据，干坏事去了，所以，用户会要求把这张证书给吊销了。吊销以后什么情况？如果有人用这证书，浏览器当然就有警告，这个是为了保证用户的密钥安全。很可惜，我前面说了，美国把它当作制裁工具了，这个很危险！这是技术滥用！

那证书过期是什么样的？证书过期是用不了的。目前证书有效期是一年，如果过期了还没续期，就会有警告，也一定要警告，为什么？因为证书过期就是无效证书了，不可能再信任它。证书有效期这块多讲两句，以前有效期是 5 年，可以签 5 年，后来，为了密钥安全改成三年，后来又改成了两年，现在是一年了。但是，谷歌今年 3 月份发布了一个公告，正在推动证书有效期缩短为 90 天，为什么要缩短到 90 天呢？是因为有效期太长保证不了 HTTPS 加密安全。因为公钥是暴露在互联网上的，而现在的云计算能力很强，包括量子计算都很强，密钥暴露太久了就有可能被破解，所以，证书有效期会缩短到 90 天，90 天证书怎么办？一年装证书要装 5 次，所以只能是自动化了。

再讲一下证书透明。刚才说了这个证书的信任机制，就是根认证计划，CA 已经信任你了，但是如果你乱签发证书怎么办？如果你的 CA 系统被人家黑掉了乱签发证书怎么办？谷歌实际上就是这样的受害者，已经发生多起假冒谷歌证书事件，谷歌说，这不行哦，我信任了 100 多家 CA 的根，如果错误签发证书，或者 CA 系统被黑恶意签发证书，怎么办？所以，谷歌想

在证书信任根机制外再加一把锁，就是证书透明。证书透明就是在签发证书之前必须公示，不公示浏览器就不信任。大家看一下，这张证书为什么不信任呢？因为这张证书的错误是Err_Certificate_Transparency_Required,就是这张证书没有 CT，浏览器是不信任的。这是 RSA SSL 证书的要求。国密 SSL 证书，零信浏览器采用了比较友好的提示,提示：证书不透明，没有像谷歌浏览器直接显示不安全，这是个过渡，我们计划明年也会采用谷歌一样的政策，如果你签的国密 SSL 证书不支持证书透明，也会显示为“不安全”，根信任了也没用，这是为了保障用户权益，这就是证书透明。

我们看一下，零信浏览器有一个创新就是证书透明的展示。看左边的图，把证书透明信息给展示出来，这张证书是从谷歌、Cloudflare 获得了 CT 签名数据，浏览器会解析 CT 签名数据，展示详细信息给你看。

右图是国密 SSL 证书，也一样展示证书透明信息，采用 SM2 算法，CT 是 SM2 的，这个明天会讲，我们展示 CT 信息不一样。

零信浏览器还有一个特点是展示可信身份，其他浏览器 EV 证书已经不显示绿色地址栏了，我们认为这个对网站安全是个威胁，因为用户上网需要知道这个网站的身份，一个假冒的网站，假冒银行网站，和真网站都一样有 SSL 证书，都有那把锁，那是没用的。现在不显示锁了，也是不行的。所以，零信浏览器仍然展示 EV 地址栏绿色和单位名称，看一下厦门大学这张证书是 EV 的，由 DigiCert 签发，有标识。如果这个网站不是 EV，是 DV/OV，想展示身份怎么办？

零信浏览器有一个可信网站认证服务，网站通过零信浏览器认证，会把认证数据写到浏览器中。这样，你使用零信浏览器访问中国政府网，就会在地址栏显示“中国政府”，给你展示出来。这是由零信浏览器做认证的，这是零信浏览器的一个创新服务。

我们还有很多很好的创新，如这个 WAF 展示，一个网站安不安全，除了有加密锁以外，还要看有没有 WAF，WAF 是 Web 应用防火墙，如果网站有 WAF 安全防护的话，用户会更加信任这个网站。所以，零信浏览器增加了一个 WAF 标识，明确标识出来。中国政府网就有 WAF 标识，是由白山云 WAF 提供服务。我们官网上也有 WAF 防护，阿里云 WAF 防护。

除了 WAF 防护标识外，我们还有个安全评级，把上面讲的检查那些项，如果有一项有问题的话就要扣分，没有问题就给分，评出 ABCDE 级别，让网站安全一目了然。这也是我们的一个创新。

总结一下零信浏览器有哪些优势？第一，内核版本比较新，基于 Chromium 114 版本开发，大家一定要查一下你目前用的国密浏览器的内核版本，凡是低于 112.0.5612.121 版本都是不安全的版本，112 以下版本有非常严重的 JavaScript 引擎存在类型混淆漏洞。你现在用的国密浏览器，如果是 112 以下版本，建议不要用，不安全的!它叫安全浏览器也是不安全的！同志们，

一定要看清楚，必须是 112.0.5612.121 以上版本。

第二，零信浏览器完全免费，这个很重要，很重要！RSA 密码体系和 RSA 密码算法的 SSL 证书为何垄断全世界，完全免费的四大浏览器功不可没，立了大功。同志们，没有浏览器，你怎么使用 HTTPS 加密？ 大家知不知道，NetScape 网景开发了第一个浏览器，收费的。同志们，你们可能不知道它是收费的，公司都准备上市了，但是，微软上了 IE 浏览器，免费，集成 Windows，免费使用！一下子把 NetScape 搞死了!为什么？用户需要免费上网啊。所以，我不知道现在怎么历史倒退了，现在需要普及国密，反而把国密浏览器都变成收费的浏览器！我觉得，这可以理解为这是互联网普及国密的初级阶段，就等于互联网刚开始阶段一样刚出来浏览器是收费的一样，所以，我们零信技术为了普及国密 HTTPS 加密，一上来就是干一个免费国密浏览器，完全免费的！我认为收费的国密浏览器，是格局有问题，我们要打破这个低格局，为普及国密做贡献，承担起国密普及的重任！

第三，不仅是免费的，而且是干净无广告，干净的！因为国密浏览器是在办公环境使用的，政府部门，大企业，国有企业大单位需要国密浏览器，所以这个浏览器在办公的时候冒出乱七八糟的广告出来，你让用户如何安心办公啊，对不对？零信浏览器是个免费的、干净的国密浏览器！

第四，我们是一个按照严格参考国际标准来要求国密 HTTPS 加密的，只有这样，才能保证我国的网站安全，保证国密 HTTPS 加密的安全！如果不是这样，号称所谓国密浏览器，只要是国密就正常连接，这是有问题的，这是巨大的安全隐患，不能信这样的国密浏览器！我刚刚为什么跟大家讲需要查验这些问题，如果不验，那它就不是个正常的国密浏览器！四大浏览器就是这样查验的！

第五，目前是独家支持国密证书透明，支持证书透明信息展示，证书透明这块很重要，不支持，我怎么知道证书是否用于攻击？这张证书是干什么用的，不敢公示。

第六，这是全球独创，其他浏览器都没有这个功能！拿谷歌浏览器对比一下，演示给大家看。我们把 PDF 数字签名功能也加进去了，能够实时验证 PDF 文档的数字签名，展示数字签名身份，一端多用，这个是全球独家的。

切回到浏览器看一下，CEO 博客文章 PDF 有数字签名，大家看有数字签名，会显示签名属性，会显示谁签的名，显示身份。同一个文件，拿谷歌浏览器看一下，那是什么样的？谷歌浏览器当然能显示这个 PDF 文件，没问题，但是它只是打开这个 PDF 文件，没有验证签名。我们看的是同一个文件，它没有验证这个数字签名，它只是显示这个 PDF 的文件名。这个是我们的全球独创的一个功能！下一步，我们还会把 Web 邮件加密和数字签名也加上去。

今天的讲座就到此结束，谢谢大家！

王高华

2023 年 1 月 18 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。