文档数字签名安全问题非常严重

零信浏览器此次发布的 2301 版本全面升级了内置的 PDF 阅读器功能，支持实时验证 PDF 文档的数字签名，并展示文档数字签名者的可信身份信息。笔者在测试了目前我国市场上被广泛使用的已签名 PDF 文档后，发现文档数字签名和文档签名证书的安全问题非常严重，本文就讲一讲这些问题，希望各相关单位能高度重视并及时改进。

深圳在全国率先实现了网上全流程注册公司，笔者两年前重新创业在线注册公司时就已经体验了其方便和高效，晚上在线提交申请，全流程用网银 Key 证书数字签名公司注册申请书，第二天拿到了营业执照，这个高效全数字化流程必须点赞，这也密码的威力，用密码来保障电子政务系统提供更快更好的政务服务。但是，当年当时只是感受到了真方便，并没有去研究其数字签名机制存在的安全问题，今天将讲一讲这个问题，以期进一步提升全数字化注册流程的密码应用安全，更安全地为用户提供优质电子政务服务！

现在，电子发票已经得到了普及应用，其中 PDF 格式电子发票文件的数字签名是关键，但是，使用 Adobe 阅读器打开电子发票文件时会提示“至少一个签名有问题”，笔者以前认为这只是因为 Adobe 不信任 PDF 签名证书而已。现在细细研究发现是真的不安全，是真的有问题，今天将讲一讲具体问题，以期进一步提升密码技术在电子发票的保真作用。

各种已签名的 PDF 文档存在的不安全问题可以具体总结为如下五大问题：

问题一：

文档签名证书采用非常不安全的 1024 位 RSA 密钥和使用 SHA1 RSA 签名算法和 SHA1 哈希算法

下图 1 为深圳 CA 签发的用于公司注册用法人股东签名用的组织机构数字证书，下图 2 为中国银行个人网银证书，可用于个人股东签名用；下图 3 为工商银行个人网银证书，也可用于个人股东签名用；下图 4 为农行个人网银证书，虽然公钥用的是安全的 2048 位，但签名算法是 SHA1，也可用于个人股东签名用。

图 1

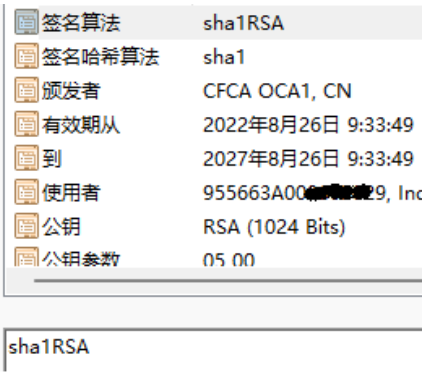


图 2

图 3

图 4

这些用于数字签名工商注册申请书 PDF 文件的数字证书采用的是非常不安全的 RSA 算法 1024 位密钥、SHA1 RSA 签名算法和 SHA1 哈希算法。国际标准组织-CA/浏览器论坛要求 2010 年 12 月 31 日**停止签发** 1024 位/SHA1 证书，并于 2013 年 12 月 31 日**禁用** 1024 位证书，如下图 5 所示。NIST 也发布了 SP 要求在 2011 年弃用 SHA1 签名和 2013 年 12 月 31 日禁用 SHA1 签名。如下图 6 所示，

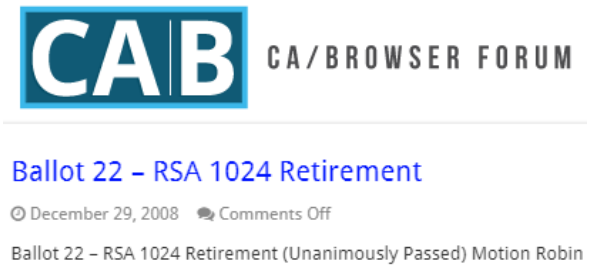


图 5

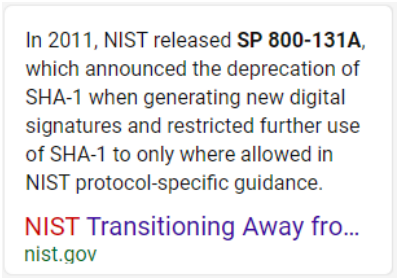


图 6

国家密码管理部门也已发过类似通知要求，但是网银系统和 CA 机构居然在国际标准要求停止签发 1024 位证书的十三年后的今天还在签发和使用！如下图 5 所示，用于工商注册用的签名证书明明是 9 月 18 日签发的，为何今天仍然提示“该证书已过期，或者尚未生效”？笔者刚开始还以为这是 Windows 提示有 Bug，但实际上国家 RSA 根证书签发给 SZCA 的

中级根证书已于 2011 年 8 月 30 日过期，这是一致 1024SHA1 证书，现在国密根官网都不再显示 RSA 算法根证书。13 年前要求禁止签发 SHA1 算法证书，13 年后的今天居然还在已经过期的中级根证书下面签发并用于数字签名公司注册和变更这么重要的法律文件！这的确是一个资深密码人不能接受的事情。

图 7

图 8

为什么要禁用？当然是因为不安全，1024 位密钥长度太短，SHA1 哈希算法也已经不安全，非常容易被破解。国际标准已经要求至少 RSA 算法必须使用 2048 位密钥长度和 SHA2 哈希算法，用安全算法签发的数字证书签发文档才能保障文档安全。

不仅有密钥不安全的问题，而且这些数字证书同时存在许多不符合标准的技术问题，包括没有 AIA 网址、没有 CRL 网址、没有授权者密钥标识符、没有证书策略、没有密钥用法和没有增强密钥用法等等，这是一张合格的数字证书必须有的字段，并且有些是关键字段，这些都没有，但是仍然用于登录网银系统认证签名用，仍然用于工商注册签名用！

问题二：

PDF 文档签名采用非常不安全的 SHA1 哈希算法和 SHA1 算法签名

这是一个如何使用文档签名证书来数字签名 PDF 文档的安全问题，目前笔者发现的无论是公司注册文 件(图 9)还是电子发票文件(图 10)的数字签名都是采用 SHA1 算法计算签名的哈希数据并采用 SHA1 签名算法的签名证书实现文档数字签名，这也是非常不安全的。

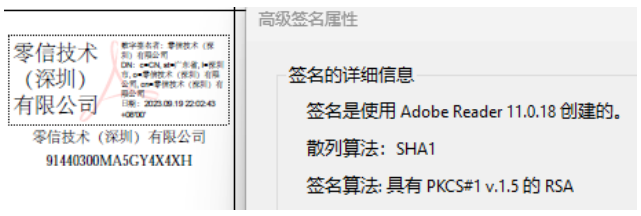


图 9

图 10

谷歌早在 2017 年 2 月 23 日就公开发布了 PDF 文档的 SHA1 哈希签名的碰撞成功破解，可以实现两个内容不一样的 PDF 文件有同样 SHA1 哈希值，也就是说一个采用 SHA1 签名的 PDF 文档可以被非法篡改内容但是数字签名仍然有效，因为哈希值不变，一样可以通过签名有效验证而不会发现已签名文件被篡改！如下图 11 所示，左边绿色部分展示两个不同的 PDF 文件用 SHA1 算法计算哈希值都应该是不同的，而右边红色部分展示的被篡改了内容的 PDF 文件的 SHA1 哈希值同原文件的 SHA1 哈希值一样。

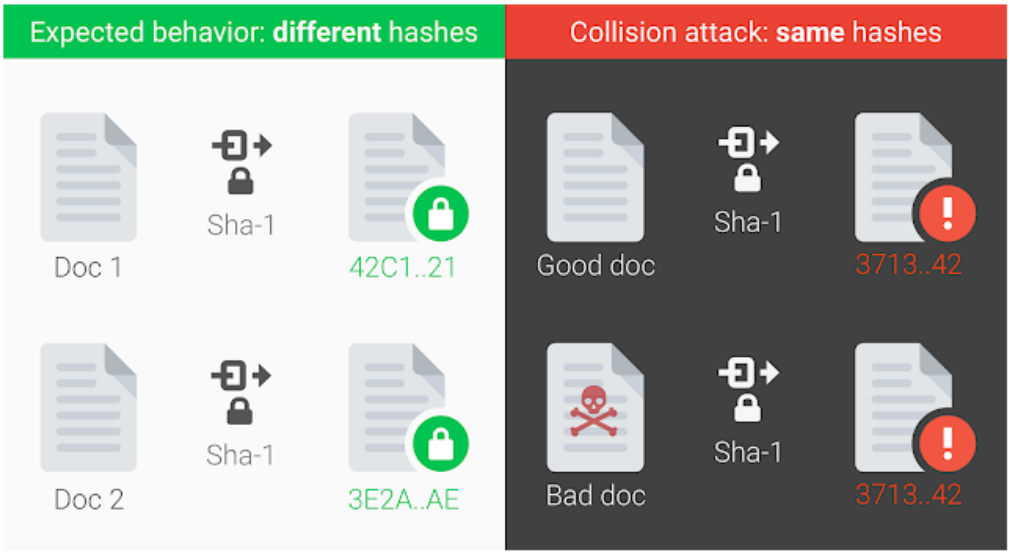


图 11

这个安全问题意味着：

(1) 采用 SHA1 计算哈希值实现的数字签名的电子发票的内容，如发票金额可以被篡改，但是由于篡改后的 SHA1 哈希值不变，所以，都能通过验签而被认为是真发票，因为使用了不安全的 SHA1 算法计算哈希值。

(2) 申请公司注册的已经签名文件，可以修改股东名称而直接把公司股权偷走，而且公司注册变更系统不会发现，因为公司注册变更系统只是验证数字签名是否有效(当然会是有效的，因为是采用不安全的 SHA1 计算哈希值)。

(3) 用户登录网银的签名和支付的数据签名可以被篡改，可以修改支付金额和收款账户等信息，但是由于能通过验签而导致偷钱成功！根源当然还是签名时使用了不安全 SHA1 计算哈希值。

(4) 采用 SHA1 计算软件哈希值已经不能保障软件的代码完整和来源，也就不能保证软件升级的安全可靠。

(5) 采用 SHA1 算法计算哈希的邮件签名(S/MIME 或 PGP/GPG)也不能保证电子邮件内容没有被篡改。

(6) 采用 SHA1 算法计算备份文件哈希的处理也不再安全。

(7) 采用 SHA1 算法的 GIT 也不能保证源代码没有被篡改。

(8) 还有许多……

问题三：

PDF 文档签名时没有带完整的证书链

这个问题同下面的四个问题跟上面两个问题比起来就显得不那么重要了，但是也必须列出来讲一讲，因为笔者发现即使用户证书采用的是安全的 2048 位/SHA2 RSA 算法文档签名证书，并且是使用 SHA2 算法实现文档签名，但是这些问题也会影响 PDF 阅读器正常验证文档的数字签名。

正常的带证书链的文档签名用 Adobe 阅读器查看是这样的，如下图 12 所示，会显示顶级根、中级根和用于签名文档的用户证书，但是笔者发现大量的电子发票签名都没有带上证书链，如下图 13 和图 14 所示，这样，即使 PDF 阅读器信任签发这张文档签名证书的根证书也没有用，因为无法构建信任链。

图 12

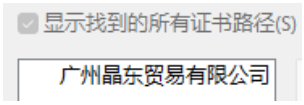


图 13

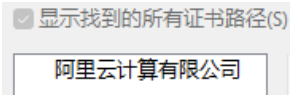


图 14

问题四：

PDF 文档签名没有附署时间戳签名

时间戳签名用于证明文档签名时的签名时间可信，如果不附署时间戳签名，则签名时间是签名服务器或签名电脑的时间，这是可以任意修改的不可信时间，时间戳对于需要证明签名时间的应用非常有用，如电子合同签署时间。笔者发现所有电子发票的签名都是没有时间戳的，公司注册文件签名也是没有时间戳的，这也是值得改进的。

问题五：

PDF 文档签名不支持 LTV(签名长期有效)

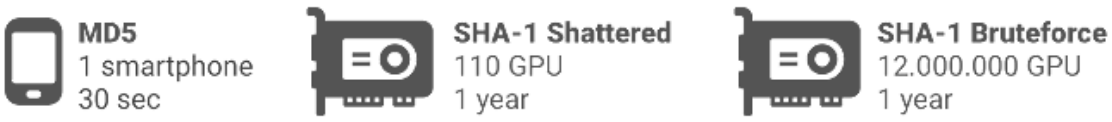
文档签名证书的有效期是有限的，最多 3 年，而文档的使用期限往往会超过 3 年，甚至是永久有效的。为了保证已签名文档的签名长期有效，在签名文档时应该支持 LTV 技术，把签名时的证书有效状态记录到 PDF 文档中以备阅读器可以查验。笔者发现所有电子发票的签名是不支持 LTV 的，公司注册文件签名也是不支持 LTV，这一项也值得改进。

问题六：

PDF 文档签名没有采用国密文档签名证书和国密算法签名

这是一个国密合规的问题，目前电子发票有用国密证书签名的案例，而公司注册文件没有发现。当然，这也是一个生态建设问题，因为 Adobe 阅读器不支持国密算法，如果电子发票和公司注册文件都采用国密证书签名的话，则需要有阅读器支持正常阅读国密签名的 PDF 文档和正常验证国密签名，需要有签名供给软件支持用国密算法实现文档签名，需要业务系统支持采用国密算法实现文档签名，和支持国密算法验证已签名文档。这个改造虽难，但是也是必须迈出的一步，早点行动早点安全合规。

以上讲解了目前我国在文档签名密码应用上的六大安全合规问题，这些问题当然不是无解的，只需业界能认识到问题所在，并积极找到解决方案去解决这些安全问题。对于问题二，大家也不用惊慌，谷歌实现的 SHA1 碰撞成功是一个特定设计的 PDF 文件，并非所有 SHA1 签名的 PDF 都可以非常容易被破解。谷歌在其安全博客中列出了一些数据：一部智能手机只需 30 秒就能破解 MD5 哈希数据，所以 MD5 哈希算法是绝对不能用的，太容易被破解了。而谷歌的特别格式 PDF 文件 SHA1 碰撞实验需要 110 个 GPU 费时一年才能破解成功，这也不是一般的公司所能提供的算力，并且还要看待破解的数据是否值得用这个代价去破解。而对于完全的 SHA1 哈希暴力破解，则需要 1200 万个 GPU 费时一年才能完成，这个算力可以理解为不可能，除非待破解的数据的价值超过 1200 万个 GPU 购买成本、系统运行成本再加上相关人力成本。



所以，现在行动起来还不晚，现在就应该规划把所有采用了 SHA1 算法相关的业务系统升

级改造，以确保采用更加安全的密码算法实现文档和文件数字签名和哈希操作。具体建议的解决思路有如下对应的六点：

第一：所有文档签名证书如果需要使用 RSA 算法，则必须使用 2048 位/SHA2 算法。

这一点非常重要，对于具体以上列出的电子发票签名和工商注册文档签名，只需签发证书的 CA 机构升级 CA 系统或修改证书签发算法模板即可，这个改造非常容易，但需要尽快改造，以确保相关的数字签名应用安全。特别是用户网银 Key 证书，这些数字证书用于数字签名网银转账数据，非常关键，必须尽快升级相关证书签发系统为网银用户签发算法安全的数字证书。

第二：所有数字签名如果需要使用 RSA 算法，则必须使用 SHA2 或 SHA3 哈希算法计算哈希。

这一点也非常重要，所有应用数字签名的系统都应该尽快升级改造，只能采用 SHA2 或 SHA3 算法生成文档哈希值，并只采用 SHA2 算法签发的文档签名证书实现文档数字签名。零信浏览器这次发布 PDF 阅读器升级版本，本计划预置信任更多的电子发票签名证书签发 CA 根证书，但我们发现电子发票中一家被广泛使用的签名证书从根证书、中级根证书到用户证书全部都是采用 SHA1 算法，电子发票 PDF 文件签名也是 SHA1 算法，这么不安全密码应用是零信浏览器不能容忍的，所以只好放弃预置信任。

第三：所有 PDF 文档签名必须带上完整的证书链，以便 PDF 阅读器能正确和快速验证签名。

这一点也很重要，零信浏览器预置信任了一家 CA 签发的专用于电子发票签发的签名证书根证书，但是这些电子发票 PDF 文件的数字签名只有用户证书，并没有包含完整的证书链，这仍然由于无法验证证书链而导致这个电子发票无法通过验证而无法正确显示其数字签名。这一点同网站部署的 SSL 证书必须部署完整的证书链是一样的，以方便数字签名验证者能正确验证数字签名是否可信。

第四：所有 PDF 文档签名都应该附署时间戳，以保证签名时间可信。

这一点也非常有用，因为电脑时间是不可信，现在电子合同数字签署非常普遍，但是如果在应用数字签名时没有同时部署可信的第三方时间戳的话，则合同签署时间是不信的，可能会引起不必要的合同纠纷，这是所有电子合同签署服务提供商必须注意的，以免给自身业务带来不可控风险。

第五：所有 PDF 文档签名都应该支持 LTV，以保障文档签名长期有效。

这一点对于需要长期使用，特别是各种档案归档签名，都应该在数字签名文档时支持 LTV 技术，让已签发文档的数字签名长期有效。最可靠的 LTV 实现是在数字签名文档时附署时间戳签名，这样才能可靠地实现 LTV，确保无论使用何种阅读器都能支持文档验证签名长期有效。

第六：这是最重要的一点，必须普及应用国密算法实现文档数字签名。

我国《电子签名法》和《密码法》都要求所有数字签名必须商用密码来实现各种数字签名和安全认证，但是，这个要求在最重要的政务系统和网银系统都还没有落实，这值得相关单位高度重视。为什么必须用商用密码算法来计算哈希和实现数字签名，当然是因为 RSA/ECC 算法的不可控，我们根本无从知晓采用的 SHA1 算法是否真的还是比较安全的，而如果真的不安全，那后果是非常严重的。唯一的解决方案是尽快采用国产密码算法来计算哈希实现各种数据的数字签名。

而要普及应用商密算法实现文档数字签名，则需要相关的生态产品都必须支持商密算法，零信浏览器 PDF 阅读器将在下一个版本支持验证国密算法 PDF 文档数字签名和提供国密算法文档数字签名服务，以期能为普及商密算法文档数字签名做出应有的贡献。

有诗为证：

文档安全靠签名，

算法选对是关键。

商用密码保安全，

生态建设最重要。

王高华

2023 年 10 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。