什么是 LTV？如何让文档数字签名长期有效？

如果读者朋友用百度搜索“什么是 LTV”或“LTV”，得到的结果有多种解释，所以特先告知读者朋友，今天所讲的“LTV”是一个文档数字签名技术名词，是英文“Long Term Validation”的缩写，意思是告诉用户此文档的数字签名长期有效。

大家用 Adobe 阅读器打开 CEO 博客的文章的 PDF 文件，点击“签名面板”都会显示下面的信息，其中有一行显示“签名已启用 LTV”，如下图 1 所示。而使用零信浏览器查看时，会显示“签名已启用严格 LTV(长期有效)”，如下图 2 所示。本文讲一讲为何我们会做这样的修改。

图 1

图 2

大家都知道，所有数字证书都是有有效期的，文档签名证书最多也是 3 年有效，而一个文档可能需要保存多年，超过 3 年，甚至需要永久保存。那么，如果文档签名证书过期了怎么办？签名证书过期了还能保证已签名文档能正常显示和验证签名吗？数字签名还能有效吗？

为了满足这个应用需求，Adobe 就发明了 LTV，在文档签名时把 LTV 参数直接加到已签名文档中，来证明此文档数字签名**时**用于数字签名此文档的文档签名证书是有效的，这个“时”就需要有一个时间依据来判断和确认当时签名时文档签名证书是否已过期和查询吊销列表来判断签名证书是否已被吊销，把这个时间点的签名证书状态信息写入已签名文档中存档，就可以用于以后判断数字签名是否有效了。

那么，为何 Adobe 阅读器显示的“签名已启用 LTV”，零信浏览器 PDF 阅读器要改为“签名

已启用严格 LTV(长期有效)”呢？首先，加上“(长期有效)”是为了用户体验，让用户一眼就明白 LTV 就是长期有效。而为何要加上“严格”二字呢？这就要回到上一段的话题，既然是要判断是否长期有效，这个关键是签名时间点，这个时间点是否可信就很关键了。

大家再看看下图 3，这是 Adobe Sign 提供的文档签名服务签名的文档在 Adobe 阅读器中所显示的签名信息，请注意最下面的一样显示“签名已启用 LTV”，再请注意其上面的一行“签名时间来自签名者计算机上的时钟”，则就是告诉用户判断当时是依据签名者的计算机时间来判断签名证书是否过期的，也是根据签名者计算机的时间来查询当时的吊销列表的。但是，请注意：签名者的计算机时间是不可信，签名者可以随意修改这个时间，也就是说，用一个不可信的时间来判断一个已签名文档的签名是否可信，这本身是一个不可信的判断逻辑，因为签名者可以修改签名时的计算机时间，即使时签名证书已过期或者被吊销，都是可以完成数字签名并写入 LTV 数据的。那么，为何 Adobe 阅读器信任这个数据而显示已启用 LTV 呢？笔者查了许多资料才发现其中的奥秘。如下图 4 所示，Adobe 阅读器的首选项设置中有“控制签名的验证方式和验证时间”设置，默认的验证签名时使用“签名的创建时间”，这就是签名者计算机时间。也就是说，Adobe 阅读器默认信任签名者的计算机时间，这样就能正常显示 LTV 信息了。这也许是 Adobe 采取的一个折中方案，方便没有附署时间戳的文档也能支持 LTV。也可能是为了照顾自己的 Adobe Sign 业务，因为 Adobe Sign 电子签名服务并没有使用时间戳签名。

图 3

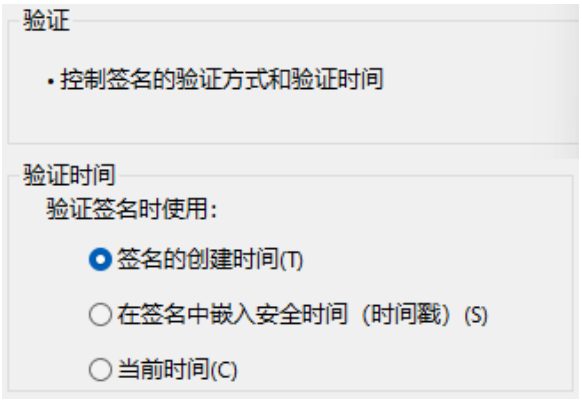

图 4

如果把 Adobe 阅读器中的默认的验证签名时使用“在签名中嵌入安全时间戳”，则原先能正常显示 LTV 的文档，会显示为“签名未启用 LTV”，已签名文档将在签名证书过期后失效。如下图 5 所示。而对于签名证书已经过期的已签名文档，则显示为“签名者的身份无效，因为其已过期”，如下图 6 所示。而如果改为默认的验证签名时使用“签名的创建时间”，则图 6 的文档会正常显示 LTV 信息。

图 5

图 6

以上讲述的是 Adobe 阅读器对 LTV 属性的展示情况，对于没有时间戳签名但有 LTV 数据的已签名文档，零信浏览器 PDF 阅读器也默认采用了 Adobe 一样的策略，也一样会显示已启用 LTV，如下图 7 所示。但是，对于已使用时间戳签名和 LTV 数据的已签名文档，如下图 8 所示，零信浏览器则显示“签名已启用严格 LTV”，这是业界首个提出的“严格 LTV”概念，因为这个 LTV 的签名时间点的时间来自受信任的时间戳签名，是可信时间，这是更加严格的 LTV 验证，所以，零信浏览器给了一个不同的状态标识-严格 LTV，类似于 HSTS (HTTP 严格传输安全，HTTP Strict Transport Security)，这才是真正可信的 LTV，因为 LTV 依赖的时间点是可信的时间戳，而不是用户电脑时间。这样，无论 Adobe 阅读器的验证时间怎么设置都一定会显示“已启用 LTV”。

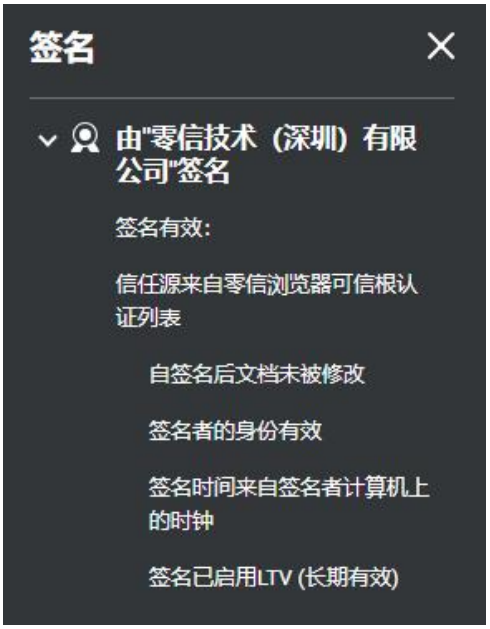

图 7

图 8

相信读者朋友已经明白了在签名文档时加上时间戳的重要了，加上时间戳，无论用户的Adobe 阅读器如何设置都能正常显示 LTV 信息，而如果不加，则取决于用户的具体设置。这就是为何零信浏览器要区分这两种签名状态的根本原因，一个是无时间戳的文档，显示同Adobe 阅读器默认设置的 LTV 状态，一个是有时间戳文档的严格 LTV 状态，无论用户怎么设置都支持 LTV 长期有效验证。

总结一下，为了确保已签名的文档长期验证有效，在数字签名 PDF 文档必须支持 LTV 方式签名。而为了让 PDF 阅读器无论用户怎么设置都能确保 LTV 长期有效，则必须在数字签名文档时同时附署时间戳签名，这样才能支持严格 LTV，以确保真正严格地实现文档数字签名长期有效。

有诗为证：

证书有效期三年，

文档使用期多年。

今朝签名保多久？

长期有效有绝招。

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。